vnu business publications 6€ GUÍAS PRÁCTICAS

PC actual
Computer Idea

PISTAS Y TRUCOS

WIRELESS ▶ VoIP ▶ TV y STREAMING DE AUDIO

¡NUEVO DISEÑO!

CONFIGURA TU PROPIA RED DOMÉSTICA

NAVEGACIÓN RÁPIDA E INALÁMBRICA

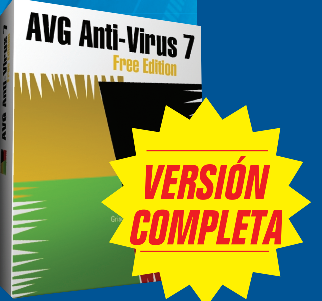
STREAMING EN TU SALÓN

LLAMADAS BARATAS ON-LINE

OPTIMIZA Y PROTEGE TU RED

CONFIGURA TU PROPIA RED DOMÉSTICA





▶ AVG ANTI-VIRUS 7 FREE EDITION
SUSCRIPCIÓN GRATUITA DE 12 MESES*

* Necesario el registro on-line gratuito después de seis meses

skype



▶ ESPECIAL FIREFOX
LOS 44 MEJORES PLUG-INS

▶ ESPECIAL SKYPE
10 PLUG-INS IMPRESCINDIBLES



vnu business publications



FIREFOX SPECIAL

Los 44 mejores plug-ins

SKYPE SPECIAL

v1.4 y v2.0 beta MÁS sus 10 principales plug-ins



7 Versiones Trial

- Dantz Retrospect 7 Professional

Retrospect protege los PCs de la pérdida de datos causada por virus, software recién instalado, errores de usuario, hardware defectuoso, actualizaciones de hardware, hackers, etc.

- CyberGauge 6.5
- EMCO Network Management 2.0
- LapLink everywhere 4
- MegaPing
- O&O Defrag V8 Server Edition
- TracePlus Ethernet v3

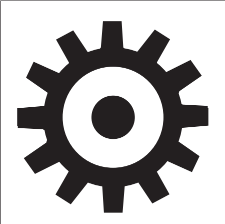
Si se ha perdido el CD, llama a VNU Publications España al teléfono: 913 137 900

CÓMO USAR EL CD

Simplemente introduce el disco en tu lector de CD, debería arrancar automáticamente. El navegador off-line ofrece la mejor opción para instalar los programas sin necesidad de dirirgirnos a las cajas de diálogo para descargar o abrir.

60 Herramientas para redes

- 3D Traceroute 2.1.8
- Abilon 2.5
- Activity Monitor 3.8
- AirSnare 1.2.11
- AnoNet 1.30
- ApSniff 0.2
- AutoDialUp 3.6
- Bandwidth Controller Lite 2.4
- Copernic Agent Basic 6.12
- DFUeTweaker 1.005
- Diskeeper 10 for Networks
- Down2Home 1.3
- Ethereal Network 10.13
- FastNet 4.3
- FileZilla 2.2.17
- FileZilla Server 0.9.11
- FPort 2.0
- Fresh Download 7.42
- Gaim 1.5.0
- Getleft 1.2a1
- Grabit 1.5.3
- HTTrack 3.33
- IE Privacy Keeper 2.7.3
- IEguard 1.0
- InternetSammler 1.7
- Internet TV & Radio-Suite Free
- Jana-Server 2.4.6.1
- Java Anon Proxy (JAP) 00.05
- Jetico Personal Firewall 1.0
- JNetTool 0.4.0
- LeechGet 2005 1.5
- Look@LAN 2.50
- WiFi Manager 4.2.1
- Maxthon 1.25
- Miranda 0.4
- Mobile Net switch 3.41
- Mozilla 1.7.12
- Netstumbler 0.4.0
- NVU 1.0
- Online TV 2.4
- Personal FTP Server 4.46
- Poppy 5.5.0
- PowerGrab 2.6
- Query Application 1.06
- Racoonworks SpeedTest 1.4
- RealVNC 4.1.1
- R-Firewall 1.0.53
- Routercontrol 1.60
- RSS-Owl 1.2
- Sitekeeper 3.5
- Skype 1.4
- SP Network Scanner 2.6
- StarDownloader 1.44 Free
- StationRipper 2.25
- Streamripper 1.61.17
- SuperGravity 2.6
- Surfmusik 3.1
- Trillian 3.1 Basic
- Undelete 5.0 Server Edition
- WatchDog 1.0
- WinXP Support Patch for WPA
- WinPatrol 9.8
- ZoneAlarm Free 6.1.737



Redes Domésticas

Contenido









Capítulo 4



Capítulo 5



Capítulo 6



La red es el nuevo centro de ocio en casa



"XP ha sido el impulsor para que las redes ocupen un primer plano"

Hubo un tiempo en que se precisaba un software especial como Novell Lite para unir ordenadores entre sí. La conexión a Internet era por entonces una ilusión imposible. Fue la aparición de los módems y de los adaptadores RDSI la que preparó el camino. Pero cada módem era diferente y lo mismo sucedía con cada versión de RDSI. Pero las cosas comenzaron a cambiar un poco con la aparición de Windows 95. Todavía resultaba extraño ver que todos y cada uno de los integrantes de una red tuvieran acceso a Internet, porque esta tarea tenía que ser gestionada por un software adicional o a través de servidores Linux unidos por un router. Windows XP ha obrado el milagro. En la actualidad, las fronteras entre las redes locales y la World Wide Web son cada vez más difusas. Las aplicaciones de red permiten, a su vez, nuevas aplicaciones como el *streaming* de audio y de vídeo. Un PC puede ser ahora cableado a un televisor o a una cadena Hi-Fi.

Por supuesto existen contrapartidas, con riesgos de seguridad ante ataques de virus o de hackers y otros retos que están por superar. El gran salto cualitativo ha llegado de la mano de las redes inalámbricas que nos liberan de las cadenas y nos hace autónomos y autosuficientes para poder acceder a la información en cualquier momento y lugar.

Si quieres realizar el viaje al mundo de las redes domésticas, acompáñanos en las páginas de esta guía en las que conocer todo lo relacionado con las redes WLAN, el presente y futuro de las conexiones de red.



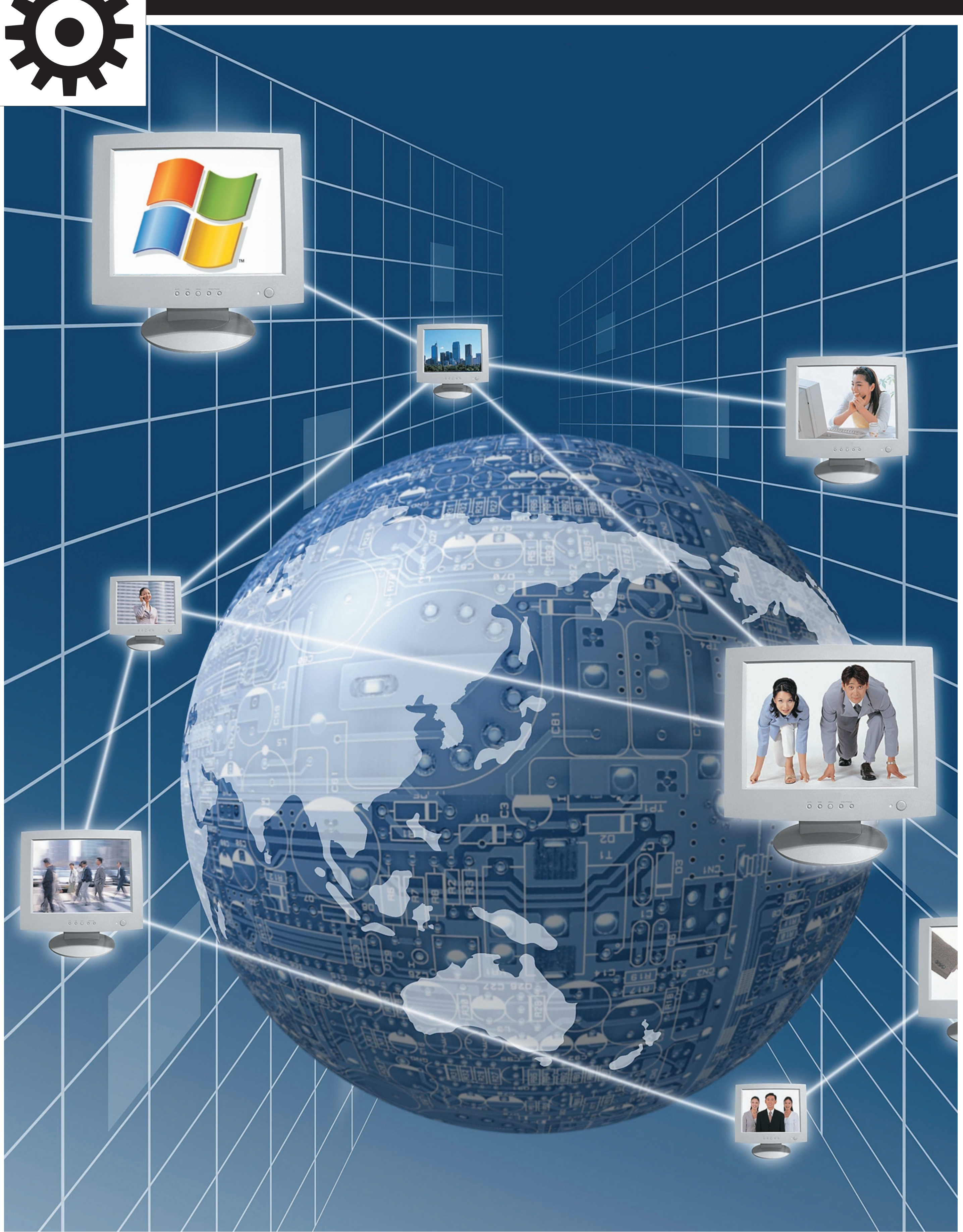
Todo lo que necesitas saber para obtener una imágenes digitales satisfactorias. Incluimos trucos para capturar, optimizar y organizar nuestras fotos. Sólo 6 euros.



Consigue que tu sistema vaya más rápido con este especial . El CD que lo acompaña incluye la versión completa de Ashampoo WinOptimizer 2005. Sólo 6 euros.



El mundo de la edición de vídeo y la grabación DVD paso a paso en esta colección de trucos, acompañada por un CD con aplicaciones imprescindibles. Sólo 6 euros.



NAVEGA EN LA RED SIN LÍMETES

Las redes inalámbricas suponen el acceso a Internet desde cualquier lugar. Examinamos los últimos desarrollos y la libertad que aportan. Tenemos páginas de consejos prácticos, así como prácticos para ayudarte a arreglar las cosas cuando fallen.

Internet sin fronteras y con velocidades inesperadas

Las redes sin cables han revolucionado el acceso a Internet. Ya es posible navegar desde cualquier rincón de casa, en una cafetería o un avión a velocidades antes impensables.

Una red de área local inalámbrica (WLAN) es la forma más óptima para instalar tanto en casa como en la oficina. Con nuestro PC compartiendo datos vía radio no nos tenemos que dedicar a la molesta tarea de montar cables. Desde cualquier punto de tu hogar, cualquier habitación, tendrás acceso a Internet. Incluso si te encuentras desplazándote de un sitio a otro. Cada vez más restaurantes, hoteles y bibliotecas públicas ofrecen puntos de acceso para conectarte y empezar a navegar al instante. Las redes de trenes y los aeropuertos también están actualizándose. Como dato interesante, la compañía norteamericana National Airlines ofrece a sus pasajeros la oportunidad de disfrutar del acceso en vuelos de larga distancia.

LOS PORTÁTILES SIN TARJETA WIRELESS YA ESTÁN OBSOLETOS porque sólo podrás beneficiarte de estas ventajas con un modelo equipado para la WLAN. Pero esto tampoco sería una traba. Los últimos portátiles con tecnología Intel Centrino incluyen de serie adaptadores WLAN. Los chipset y la tecnología inalámbrica vienen de la mano para crear la unidad portátil más perfecta. Incluso los equipos más económicos que no están basados en el procesador de Intel, están lanzándose al mercado con el correspondiente adaptador. Una forma barata de actualizarte al mundo inalámbrico es utilizar una simple llave USB WLAN. Instala los controladores en tu PC y cada vez que insertes la llave USB, empezará a funcionar como un dispositivo de envío y recepción de señales.





Navega cuando y donde quieras... United Airlines te ofrece acceso a la Web en sus viajes París-Nueva York.

"La WLAN actual es estable, segura y rápida"

TE OFRECE LA ÚLTIMA TECNOLOGÍA EN TÉRMINOS DE VELOCIDAD, SEGURIDAD Y ESTABILIDAD: La mayoría de los pequeños negocios están migrando a configuraciones de estas características pero no sólo por las molestias de los cables sino porque asegura una velocidad, rapidez y fiabilidad contrastadas.

SEGURIDAD: Gracias al método de encriptación WPA (acrónimo de Wi-Fi Protected Access y ya con el estándar WPA2), estas redes son mucho más seguras que años atrás. No resulta del todo imposible que alguien espíe nuestros datos, pero el blindaje resulta más eficaz. En realidad, te encontrarás igual de seguro tanto en un WLAN como en una red convencional cableada, siempre que la red no esté visible para el público y sólo los equipos designados tengan acceso. Los trucos de las páginas siguientes te mostrarán cómo es el funcionamiento.

ESTABILIDAD: Como todas las soluciones de radio, el alcance y por lo tanto la estabilidad de la conexión dependerá de las condiciones del edificio. Paredes gruesas entre el terminal y el *router* pueden obstaculizar la recepción de la señal. De todas formas, los sistemas modernos tienen un radio de acción de 30 metros dentro de un entorno de oficina habitual.

VELOCIDAD: El estándar actual de WLAN es el IEEE 802.11g, que puede alcanzar una velocidad máxima de 54 Megabits por segundo (Mbps). Este ratio resulta más que suficiente para la navegación web e incluso para descargas rápidas de archivos de gran tamaño.

EL FUTURO DE LA WLAN: Sólo aplicaciones críticas al tiempo, como el caso del *videostreaming* han presentado hasta ahora problemas. Este tipo de datos a menudo presentan dificultades para atravesar sólidas paredes. Mantener la señal constantemente se convierte en un problema. Esto, por lo tanto, resulta fatal para el *streaming*. Sin embargo, cuando navegamos, las pequeñas interrupciones de los sonidos o vídeos no revisten excesiva importancia.

El nuevo estándar IEEE 802.11n trae aparejadas grandes ventajas. La parte fundamental de esta tecnología se basa en la ya disponible antena múltiple MIMO (*Multiple Input Multiple Output*). Con ella se pueden conseguir ratios de datos de 108 Mbps e incluso los expertos hablan de que en poco tiempo llegará hasta los 300 Mbps. Por añadidura, MIMO hace posible conexiones más estables en largas distancias. En el futuro, seremos capaces de saber el alcance exacto de las señales entre el router y el PC en diferentes puntos de la casa. Hasta ahora, los fabricantes no han sido capaces de ponerse de acuerdo con especificaciones conjuntas. Las primeras configuraciones con MIMO abarcan los 60 metros en un entorno de oficina.

Esta nueva generación inalámbrica es tan rápida porque los dispositivos MIMO no envían y reciben las señales con una sola antena, sino con múltiples antenas. De esta manera, señales separadas de radio pueden ser transmitidas por la misma fre-



Busca el logotipo de Intel Centrino si deseas adquirir un nuevo portátil con WLAN integrada.

Estándares WLAN

Cualquiera que mezcle en un mismo entorno «g» y «b» está perdiendo definitivamente rendimiento. Para los entornos WLAN existen dos estándares de red: 802.11g y 802.11b. Con el primero de ellos, la conexión de radio se realizan en un rango de transferencia de 54 Mbps, mientras que el más débil 802.11b suministra tan sólo 11 Mbps. Los dos sistemas utilizan una frecuencia de 2,4 GHz y ambos pueden convivir en una misma red.

En estos casos se produce un efecto ralentizador en la red. Los dispositivos b reducen el rango de transferencia de los dispositivos g hasta un 50 por ciento. Y esto se produce incluso si sólo hay un dispositivo b conectado al punto de acceso e incluso sin que se estén transmitiendo datos. Esto es debido a la carga de trabajo que se ocasiona dentro del punto de acceso al tener que gestionar dos estándares en vez de uno. Para paliar este efecto, es aconsejable adquirir tarjetas de red con Nitro, una herramienta que incrementa considerablemente la velocidad dentro de las redes mixtas.

Nitro permite transferir más paquetes de datos 802.11g que el propio estándar, y según aseguran muchos fabricantes se produce un incremento de velocidad próximo al 50 por ciento. En un banco de pruebas de nuestro Laboratorio lo máximo verificado ha sido una mejora del 20 por ciento, que no deja de ser un dato interesante. La pega es que pocos proveedores ofrecen tarjetas Nitro, aunque todo apunta a que la oferta irá creciendo.

cuencia manteniendo la integridad de la información. Esto incrementa el tráfico de datos sin ocupara otra frecuencia de radio y sin interferir con otros dispositivos de radio. El rango se incrementa gracias a la combinación de señales.

Las partes metálicas de un edificio de la antena pueden producir rebotes de señal, y esto explica por qué una misma señal llegar al mismo ordenador en momentos diferentes. La nueva tecnología empaqueta estos fragmentos en una única señal.

ALTA VELOCIDAD PARA HOY: Para aquellos de nosotros que no podemos esperar a que la nueva tecnología esté disponible, conviene saber que existen antenas múltiples. Importantes fabricantes como NetGear, Asus o Gigabyte ofrecen ya modelos que van desde 125 a 250 euros. Con ellos no tendremos ningún problema a la hora de disfrutar de *streaming* de vídeo. La velocidad de 108 Mbps suministrada por un router con antena múltiple es lo suficiente potente para transmitir vídeo sin tirones. La reducción de la vulnerabilidad de las interrupciones permite una tasa estable de datos y, como consecuencia, el suministro de sonido e imagen de calidad. Son adecuadas para distancias de 20 metros o más.

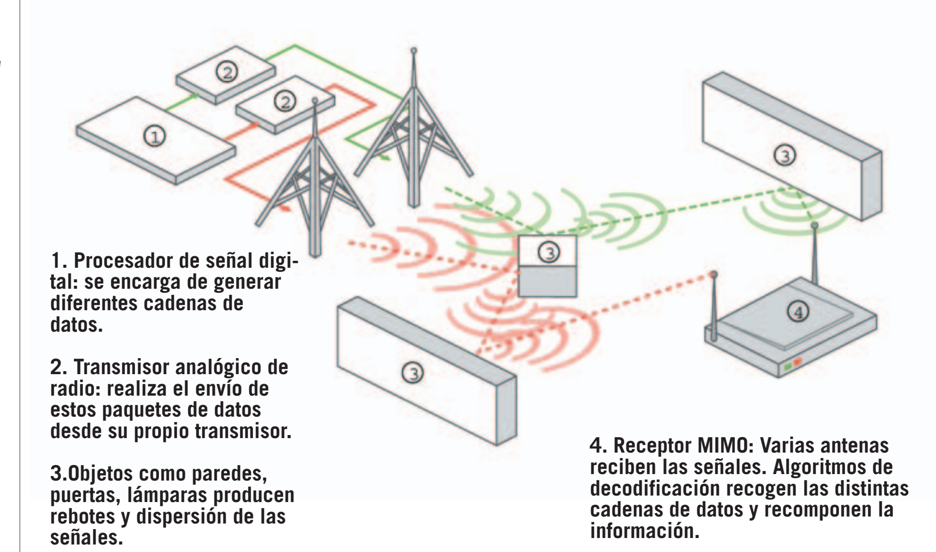
AGUJEROS DE SEGURIDAD EN VIEJOS Y NUEVOS ROUTERS: Si estás interesado en adquirir un router de última generación, tienes que prestar atención al método de encriptación. No sólo debe soportar el estándar WEP (Wireless Equivalent Privacy), sino WAP (o mejor, WAP2). Algunos modelos ofrecen WPA con





Linksys ofrece un kit MIMO WLAN que contiene un receptor y una tarjeta PC que nos permite actualizar incluso portátiles antiguos.

Guía visual de MIMO



1. Procesador de señal digital: se encarga de generar diferentes cadenas de datos.

2. Transmisor analógico de radio: realiza el envío de estos paquetes de datos desde su propio transmisor.

3.Objetos como paredes, puertas, lámparas producen rebotes y dispersión de las señales.

4. Receptor MIMO: Varias antenas reciben las señales. Algoritmos de decodificación recogen las distintas cadenas de datos y recomponen la información.

Pistas rápidas para WLAN

Wireless Network Connection (FRITZ!Box Fon WLAN 7050)
Speed: 24.0 Mbps
Signal Strength: Excellent
Status: Connected

Calidad de conexión: Antes de realizar descargas superiores a los 10 Mbytes, debes siempre chequear la calidad de la conexión. Para hacer esto, mantén el cursor del ratón sobre el icono de la conexión WLAN en la bandeja del sistema, en la parte inferior de tu pantalla. Windows mostrará una pequeña ventana en donde se indica el *status* de la conexión.

Conexiones a Internet separadas: Si un número de ordenadores están compartiendo una red WLAN, el ancho de banda es compartido a su vez. Si estás navegando, escribiendo o chequeando *e-mails*, es raro que percibas el descenso. En cambio, el *streaming* de vídeo o la descarga de archivos «pesados» requieren que el resto de los usuarios no se encuentran realizando tareas similares.

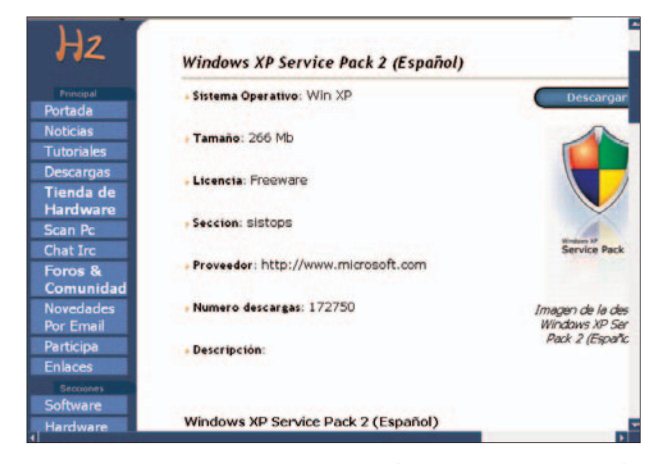
Adaptadores USB: La empresa Belkin cuenta con un adaptador USB rápido bajo el estándar 802.11g: USB 2.0 Network Adapter. Esta pequeña llave puede usarse tanto en redes b como en redes g y soporta la versión rápida USB 2.0. El precio de este producto ronda los 30 euros (www.belkin.com).

Cheque la seguridad: Puedes chequear si el firewall del router es realmente seguro utilizando un test *on-line* como por ejemplo www.security_space.com. Encontrarás una herramienta totalmente gratis en la dirección http://scan.sygate.com



Un adaptador rápido WLAN es fácil de instalar. Lo único que necesitas es algo tan común como un puerto USB.


Las AirStations de Buffalo cuentan con tecnología de antena múltiple que permiten enviar datos de forma más rápida y fiable.



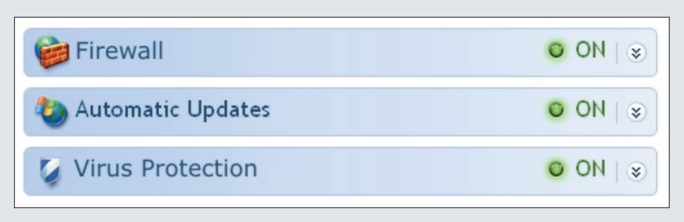
Microsoft ofrece una actualización gratuita de su SP2.

la variante TKIP (*Temporary Key Integrity Protocol*), que está basado en el mismo hardware como el viejo e inseguro WEP. WAP2 está diseñado bajo los aceptados y eficaces algoritmos AES (*Advanced Encryption Standard*). Utiliza este método si tu router lo soporta. Deberás también actualizar Windows XP. En el centro de descargas de Microsoft (**www.microsoft.com/downloads**) simplemente teclea sobre la palabra clave KB893357 y accederás a la ventana de bajada de los archivos y comienza la instalación.

ACELERACIÓN DE DATOS SIN COSTE: Si no deseas esperar a la nueva generación WLAN, no tienes que resignarte a sacrificar la velocidad. Tanto usando herramientas integradas de Windows como una buena cantidad de freeware, puedes alcanzar una aceleración de la tasa de transferencia datos. Esta tarea se realiza en tres pasos. Primero tienes que encontrar el lugar óptimo para tu router ya sea en tu oficina o en tu hogar. La potencia real de transmisión es más importante que la orientación. Deberás probar diferentes puntos de acceso durante varios días. En oficinas grandes y en las casas, reconocerás con facilidad las diferencias de calidad de recepción. Ahora configura tu router para adecuarlo a tu infraestructura. Aquí surge un consideración: si estás utilizando solo la WLAN o alguien más comparte el acceso contigo, pues necesitarás eliminar o deshabilitar algún componente o servicio de Windows. También tendrás que configurar Internet Explorer, lo que te dará conexión gratutita y te permitirá navegar más rápido. ■

Localización del router: Elementos metálicos y el hormigón de algunas paredes pueden desviar la señal proveniente de un router WLAN. Para obtener la mejor conexión, no deberás situar el router y el ordenador entre paredes gruesas. Si no se trata de dispositivos de infrarrojos, no será tampoco necesario que se encuentren ambos a la vista.

Service Pack 2: Sin ninguna duda, debes instalarte el Service Pack 2 para Windows XP y activar todas sus funciones de seguridad, incluyendo el firewall y las actualizaciones automáticas. En el caso de convivir dos firewalls (nunca dos de software) en un mismo sistema, el firewall de hardware de tu sistema y el de XP no se afectarán entre sí.




Ten cuidado. Los microondas pueden interferir y afectar directamente en la recepción de señal.

Puntos de acceso público: Los *hotspots* públicos son útiles, pero no confíes en ellos ciegamente. La realidad es que nunca se sabe a ciencia cierta si la conexión es segura o si tus datos están siendo utilizados. Con esto claro, nunca realices banca *on-line* o envíes mensajes confidenciales con este tipo de conexión. Utilízalos sólo para navegar.

Problemas de radio: Si una transmisión de vídeo se desconecta de repente o baja la velocidad del streaming, la presencia de un horno microondas puede ser la fuente del problema. Cuando lo utilizamos, el microondas utiliza un rango de frecuencia de 2,4 GHz que puede incidir en tu red. Ambos deben hallarse lo más alejados posible.



Conéctate sin cables al gran mundo de la Red

Navegar sin cables es una experiencia verdaderamente liberadora. Sin embargo, debes vigilar la seguridad con independencia de tu ubicación.

Controla el acceso WLAN »

Dirección MAC

Utilizando una lista de control de acceso, podrás decir al router cuáles son los ordenadores que pertenecen a tu red. Esta lista se confecciona en base a las direcciones MAC (Control de Acceso Multimedia) de los adaptadores de red. Cada dirección existe globalmente sólo una vez. Si la registras en tu router, ningún otro PC podrá acceder a la red. La dirección MAC suele venir anotada en una etiqueta pegada al adaptador de red; si no es así, determínala de la siguiente manera: en la carpeta de *Conexiones de Red*, haz clic en el botón derecho sobre *Conexiones Inalámbricas* y después pincha en *Estado*. Cambia a la pestaña de *Soporte de Red* del cuadro de diálogo y pincha en *Detalles*. La dirección MAC de tu adaptador de red aparecerá como una dirección física. Anota la columna de cifras. Ahora, añádela al control de acceso del router. Repite el procedimiento con cada PC que tengas en la red.

Wireless LAN- MAC-Filter

Activated: yes
Action: enable address

	Mac address		
1	00:03:2f:18:90:99	2	00:60:b3:91:a1:87
3	00:04:23:85:64:ba	4	00:0c:f1:35:07:95
5	00:0a:95:f2:06:9f	6	00:04:23:85:63:c0
7	00:a0:c5:b7:3a:2e	8	00:0f:c9:01:49:78
9	00:a0:c5:5c:5b:c3	10	00:01:e3:06:c4:91

Registra la dirección MAC en el software del router para permitir que los ordenadores externos accedan a tu red doméstica.

Cómo esconder el nombre de tu red a los intrusos »

Seguridad

Como si fuera una cadena de radio, cada WLAN tiene un nombre de estación único, llamado SSID (*Service Set Identifier*) o ESSID (*Extended Service Set Identifier*), que permite a los terminales de recepción identificar la red. Puedes cambiar estos nombres para distinguir las distintas redes dentro de una misma área de recepción, pero es mejor esconder la red de cara al exterior. Sólo tendrás que desactivar en el router la opción llamada *Broadcast SSID* o *Broadcast ESSID*. En lo sucesivo, la red será solo visible a los ordenadores cuyo nombre aparezca registrado en las propiedades de red.

Wireless LAN- Wireless

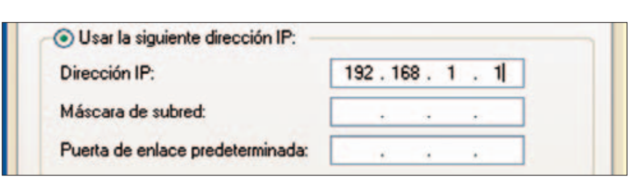
- [x] Activate Wireless LAN
- ESSID: Mingo
- Hide ESSID: yes (no / yes)
- Channel: 2462MHz
- [ ] Limit RTS/CTS: 2432 (0 ~ 2432)
- [ ] Limit fragmentation: 2432 (256 ~ 2432)
- WEP encryption: 128 Bit WEP

Esconde el SSID para que tu WLAN no sea localizada o espiada por receptores extraños.

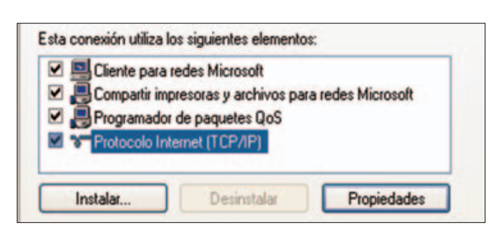
Arranca más rápido sin DHCP »

Igual a igual

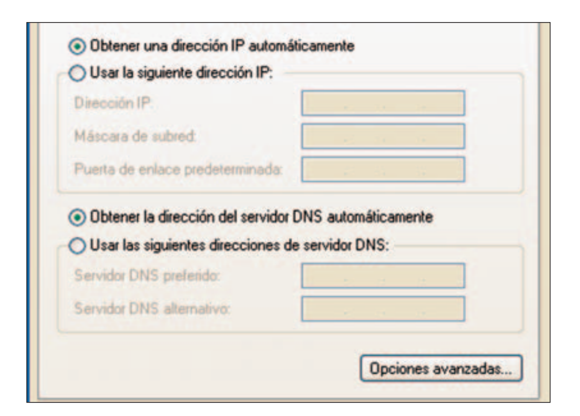
Los sistemas que empiezan con una inicialización de red son mucho más rápidos sin el DHCP. Esto es así si se utiliza la WLAN como una intranet, sin estar conectada a Internet (por ejemplo, en redes igual a igual). En este caso, asigna una dirección IP fija a todos los ordenadores conectados a la red. Tiene que estar dentro de los valores 192.168.0.x y 192.168.255.x. Abre la ventana de *Propiedades de conexión de red* y cambia a la pestaña *Conexiones*. Sitúa el cursor en la opción *Protocolo Internet (TCP/IP)* y pincha en *Propiedades*. Abre la pestaña *General*. Selecciona la casilla *Utilizar la siguiente dirección IP*. Como dirección, introduce uno de los valores mencionados antes; pero ten en cuenta que cada dirección IP puede existir sólo una vez en la red.



Si utilizas una dirección IP fija, Windows no tendrá que encontrar y manejar datos de la red al iniciarse.



Las configuraciones de la DHCP pueden ser revisadas en las propiedades del TCP/IP. Lo más aconsejable es que Windows obtenga la IP y la DNS de forma automática



Sintonizar el router con el PC »

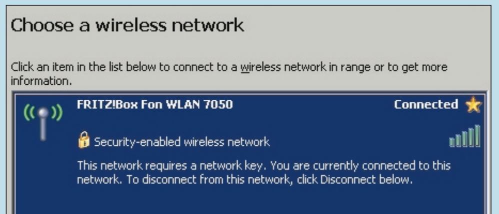
Configuración de DHCP

Si se producen problemas con la asignación de la IP, Windows informará de que la conexión es limitada. Este error aparece si las configuraciones del DHCP del router y las del PC no concuerdan. Asegúrate de que la DHCP está activada. Pincha en *Mis sitios de red* y después en *Ver conexiones de red*. Ahora, introduce las propiedades de tu red inalámbrica, marca *Protocolo Internet (TCP/IP)* y *Propiedades*. En la siguiente ventana, elige *Obtener una IP automáticamente* y también *Obtener una DNS automáticamente*. Si la DHCP se ha configurado correctamente en tu PC, revisa el adaptador de red. Abre el *Panel de control* de Windows y haz clic en *Sistema*. En la pestaña de *Hardware*, pincha en *Gestión de Dispositivos*. Si muestra algún error con el adaptador de red, reinstala o actualiza el controlador del dispositivo. Pero el problema puede deberse al router. Lee el manual del router para saber cómo resetearlo. Normalmente, los routers cuentan con un botón en la parte de atrás que debe ser presionado unos segundos para devolver el dispositivo a su estado original.

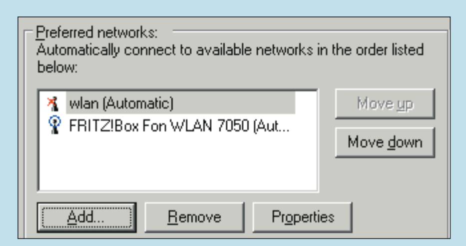
Llamadas automatizadas »

Problemas de conexión

Si el mensaje *Obteniendo dirección de red* se mantiene más tiempo del habitual, el ordenador no podrá encontrar una red a la que conectarse. Habrá, seguramente, varias WLAN disponibles, así que asegúrate de que tu ordenador intenta conectarse sólo a tu red preferida y a ninguna otra. Abre el cuadro de diálogo de *Conexiones de Red*, haz clic en el botón derecho sobre *Conexiones de red inalámbricas* y después en *Ver Redes inalámbricas disponibles*. Ahora,



Windows no puede actualizar la lista de redes disponibles él solo.



Es posible quitar las conexiones WLAN no deseadas del sistema para prevenir problemas con las llamadas automatizadas.

selecciona *Configuraciones Avanzadas*, *Redes inalámbricas* y marca tu conexión como red preferida. Pincha el botón de la flecha hasta que tu red se sitúe en el primer puesto de la lista. Asegúrate de que todos los datos de llamada están bien. Marca el nombre de la red y pincha en *Propiedades*. Revisa la SSID registrada. Por último, cambia a la pestaña de *Conexiones* y marca la casilla de *Conectar cuando esta red esté disponible*.



El bloqueador de elementos emergentes de Service Pack 2 te libera de ventanas indeseadas a la vez que define excepciones para aquellas páginas que pueden contener información importante (de tu banco, por ejemplo).

Denegar el acceso a anuncios »

Elementos emergentes

Los anuncios emergentes no son sólo engorrosos, además nos hacen perder mucho tiempo para cerrarlos. Afortunadamente, existen unas cuantas herramientas gratuitas que te ayudarán a deshacerte de ellos. Webwasher (www.webwasher.com) es un buen ejemplo (gratuito sólo para usuarios privados). Puedes también deshacerte de los anuncios desactivando los Java Script en Internet Explorer. Para ello, abre primero las *Opciones de Internet* en el menú de *Herramientas* y cambia a la pestaña de *Seguridad*. Haz clic en el botón de *Nivel Personalizado*. Puedes desactivar aquí los controles ActiveX. Pero hazlo con precaución: al cambiarlos, puede que bloquees otros elementos y funciones de las páginas Web que visitas. Todo esto será innecesario cuando instales Windows XP Service Pack 2, puesto que Internet Explorer viene ya con una función que bloquea los anuncios emergentes. Sus configuraciones se encuentran en el menú de *Herramientas*. Pincha en *Bloqueador de elementos emergentes* y en *Configuraciones de bloqueador de elementos emergentes*.

Ten cuidado cuando navegues en público »

Puntos de acceso

Si quieres navegar por Internet desde un punto de acceso público, por ejemplo, en el aeropuerto o en una cafetería, no olvides que en estos lugares no tienes ningún control sobre las configuraciones de seguridad y encriptación de la conexión. Normalmente, los puntos de acceso público no necesitan clave WEP. Después de registrarte, abre tu navegador. Tu web de acceso inicial será el sitio de la puerta elegida. Estos portales proporcionan una selección de opciones de autentificación y facturación. Lo ideal sería que pudieras seleccionar el proveedor más barato antes de registrarte. Algunos ofrecen un límite de horas gratuitas en estos puntos de acceso y sólo te hacen pagar si sobrepasas este tiempo. Por razones de seguridad, deberías evitar enviar archivos confidenciales desde estos lugares públicos.

Incrementar el alcance de la red »

Amplificadores WLAN

Si la recepción de tu WLAN no te satisface, puedes utilizar amplificadores como Linksys WRE54G (www.linksys.com, 70 euros) o el de Siemens, Gigaset WLAN Repeater (www.siemens.com, 77 euros). Estos aparatos funcionan como estaciones de transmisión, recibiendo y después redireccionando las señales de red. De esta forma, incrementan el alcance de la red y la cobertura de la señal en entornos desfavorables, como edificios con muchos muros internos, etc. Para que un repetidor pueda redireccionar las señales debe ser potente y estar situado dentro del alcance de la red existente. Por regla general, vienen con opciones de conexión inalámbrica.



Los amplificadores como Siemens Repeater fortalecen la señal para que la WLAN sea accesible desde las habitaciones más lejanas.

Configuración del grupo "Todas las cuentas"
- [x] Incluir este grupo en envío y recepción (F9).
- [x] Programar un envío o recepción automáticos cada 10 minutos.
- [ ] Realizar envío o recepción automáticos al salir.

Cuando Outlook no tiene conexión
- [x] Incluir este grupo en envío y recepción (F9).
- [ ] Programar un envío o recepción automáticos cada 5 minutos.

Cerrar

Marca en tu gestor de correo que compruebe el correo cada 10 minutos para evitar la desconexión por falta de uso.

Cómo evitar una desconexión forzada »

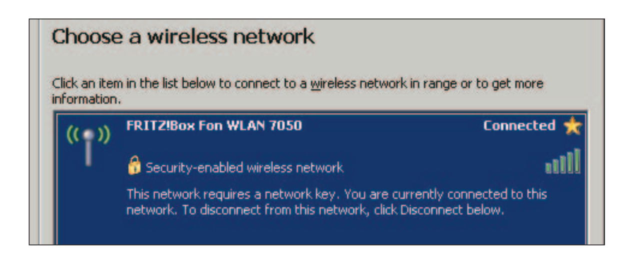
Sesiones online

Las desconexiones forzadas son una medida de seguridad del proveedor y no pueden ser anuladas. Para la mayoría de los proveedores, el límite de conexión está en 24 horas después de la llamada. Algunos proveedores pueden cortarte incluso a los 15 minutos de conexión. Así que, antes de empezar una descarga voluminosa, es recomendable que realices la llamada de nuevo... De esta forma, tendrás otras 24 horas antes de la desconexión. También puedes engañar al sistema con Outlook Express. Para ello, di al software de correo que revise automáticamente la recepción de mensajes cada diez minutos. De esta forma, nunca te acercarás al tiempo límite. Encontrarás la forma de configurar Outlook Express en las *Opciones* del menú de *Herramientas*.

Reiniciar puede ayudar »

Problemas de transmisión

Aunque las oficinas sin hilos son estupendas, a veces los continuos cambios en la intensidad de la señal llegan a resultar insoportables. Si tu intensidad de señal fluctúa constantemente, deberías colocar tu PC cerca del router. Casi todos los fabricantes aseguran que las conexiones de radio serán estables (incluso a través de muros y en un radio de cerca de 200 metros), pero la realidad es bien distinta. Si has perdido la conexión, lo más seguro es que se deba a un problema de configuración. En este caso, asegúrate de que el sistema reconoce la red y que el router tiene asignada una dirección IP para tu ordenador. La forma más rápida de saberlo es escribiendo el comando «ip config» dentro de la ventana de Ejecutar.

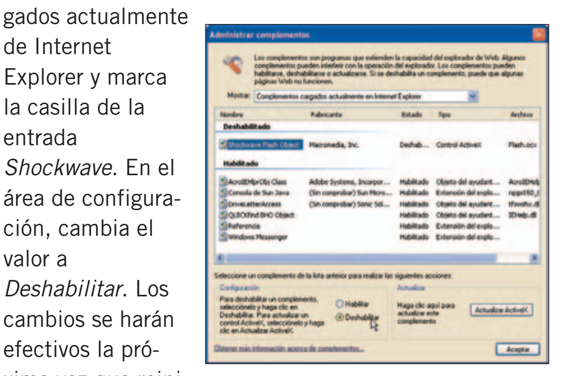


Las barras de color indican que la señal es débil. En ciertas condiciones, puedes perder la conexión.

Cómo desactivar las animaciones »

Shockwave

Si no quieres que esas aburridas animaciones de las páginas web aparezcan en tu ordenador, no tienes por qué cerrar la ventana individualmente cada vez que salen. En lugar de eso, puedes bloquearlas por completo. Para ello, pincha en Administrar complementos del menú *Herramientas* de Internet Explorer. En la casilla *Mostrar*, pincha en los complementos descargados actualmente de Internet Explorer y marca la casilla de la entrada *Shockwave*. En el área de configuración, cambia el valor a *Deshabilitar*. Los cambios se harán efectivos la próxima vez que reinicies Internet Explorer.



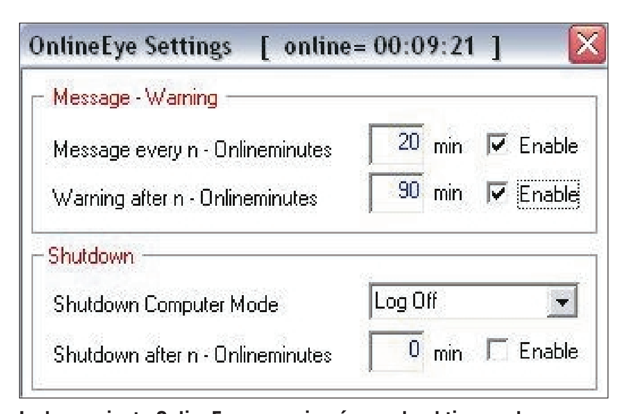
Si no quieres que te molesten las animaciones de las páginas web, deshazte de Shockwave.

Mejorando los antiguos PCs »

Dispositivos USB

Los dispositivos USB WLAN son una buena alternativa a los adaptadores WLAN porque proporcionan acceso a Internet sin cable y no necesitan la instalación de ningún hardware o software para su funcionamiento. Estos dispositivos tienen un precio inicial de unas 28 euros. Pero, ¡atención al comprarlos! Asegúrate de que soporta USB 2.0, es decir, que el ratio de transferencia desde y hasta la memoria flash es mucho más rápido que con USB 1.1. Un consejo: intenta comprar un lápiz que tenga un mango flexible. Esto es crucial con los PCs, porque te permite orientar la antena hacia el punto de acceso.

Los dispositivos WLAN USB son prácticos y baratos y permiten la conexión vía WLAN de los viejos ordenadores.



La herramienta OnlineEye nos avisará cuando el tiempo de navegación se esté acabando.

El tiempo es oro cuando se navega »

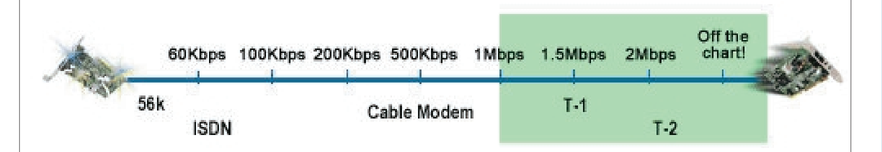
Volumen de datos

Las tarifas planas no son siempre la mejor opción. La gente que navega menos de dos horas diarias debería plantearse si le compensa. Para evaluar la transferencia media de datos mensual de una forma realista, no tienes que utilizar un reloj especial. OnlineEye, de Pmasoft (*www.pmasoft.net*) lo hace por ti. Esta herramienta gratuita registra todo el tráfico *on-line*, incluido el del correo electrónico, permitiendo al usuario conocer su comportamiento en la red. OnlineEye funciona sutilmente en la sombra, no utiliza demasiados recursos del sistema y te alerta automáticamente cuando vas a sobrepasar el tiempo que tú mismo has definido para navegar. También despliega la actual dirección IP asignada.

Comprobando tu conexión a Internet »

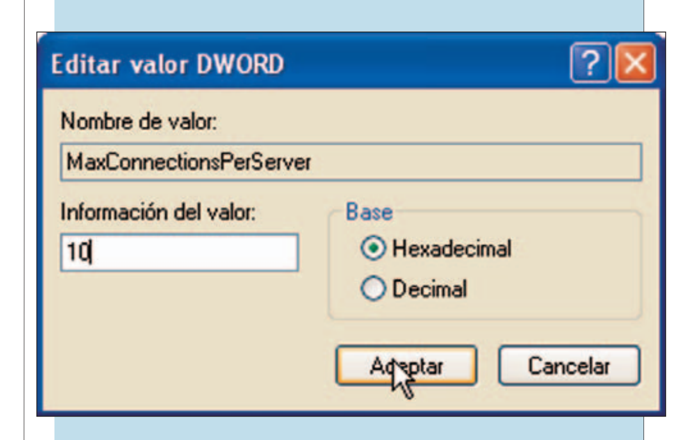
Velocidad estimada

Si quieres averiguar cómo es de rápida tu conexión a Internet, no necesitas comprar, ni siquiera emplear, un software especial. Utiliza **www.computers4sure.com/speed.asp** para medir rápida y convenientemente el uso de tu red. Este sitio transfiere una gran cantidad de datos a tu PC, mide el tiempo, y después calcula la velocidad. El proceso no lleva más de un minuto. Si quieres determinar por separado la velocidad de las descargas o de los envíos necesitarás una herramienta de gestión de velocidad. Estos programas miden la navegación, la velocidad de descarga en la sombra, y muestran después los resultados gráficamente.



Your Speed is: 1920 Kbps

Esta página web mide la velocidad actual de la línea de datos.

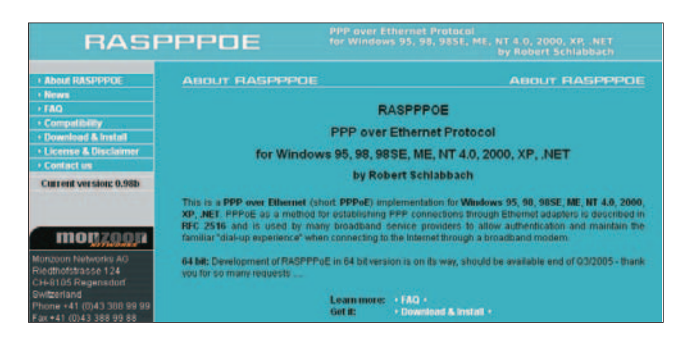


Una nueva entrada en el registro incrementa el número de descargas posibles.

Controladores que aumentan el rendimiento »

Controladores PPPoE

Remplazando el controlador de Windows PPPoE, puedes alcanzar mayor velocidad y acumular menos volumen de datos en el registro de Windows. El controlador original, por ejemplo, ignora los valores MTU más altos de 1480; los controladores gratuitos PPPoE (Protocolo sobre Ethernet Punto a Punto) como RASPPPoE (**www.raspppoe.com**) o el llamado controlador Engel son perfectos como alternativa al controlador original de Microsoft. Los controladores Engel tienen la ventaja de que con ellos puedes navegar por Internet sin necesidad de instalar ningún software de tu proveedor. Así, por ejemplo, puedes navegar con tu conexión de llamada sin instalar el software de AOL. Busca siempre la versión más nueva. Las versiones anteriores a XP necesitarán siempre un controlador PPPoE, excepto si utilizas un router. En este caso, la conexión puede establecerse directamente desde la interfaz del router porque el controlador está ya disponible.



En muchos casos, sustituir el controlador original de Windows PPPoE acelera la navegación por Internet y te evita el tener que instalar software *on-line* de tu proveedor.

Más descargas al mismo tiempo configurando el Registro »

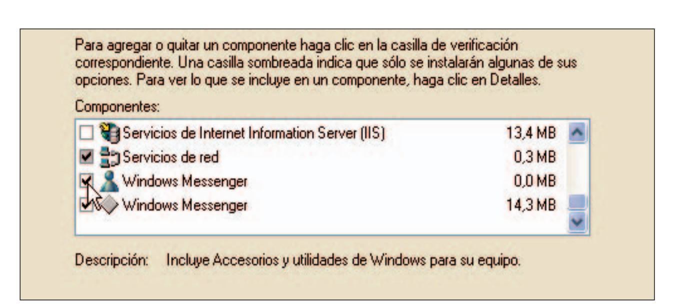
Ajuste del registro

Por defecto, encontrarás que Windows XP e Internet Explorer 6 te permiten realizar sólo dos descargas paralelas desde un mismo servidor. Pero como dueño de un módem ADSL, querrás sin duda empezar tres, cuatro o incluso más descargas al mismo tiempo. No pasa nada, lo único que necesitas son unos pequeños ajustes en el registro de Windows. Abre primero el registro haciendo clic en *Inicio*. Ahora pincha en Ejecutar, escribe *regedit* y presiona «Intro». Revisa con cuidado el registro hasta que encuentres la siguiente clave: *HKEY_CURRENT_USER\Software\Microsoft\Windows\Current Version\InternetSettings*. Para añadir una entrada DWORD nueva, haz clic en *Nuevo* del menú *Edición* y en el valor *DWORD*. Ahora, debes sobrescribir la entrada por defecto con MaxConnectionsPerServer. Una vez hayas hecho esto, haz clic en el botón derecho del ratón. Introduce un nuevo valor en la ventana de la derecha y haz clic en *Modificar*. Dentro del nuevo cuadro de diálogo, cambia la configuración por defecto de hexadecimal a decimal y bajo el *Valor* establece el número máximo deseado de descargas, digamos, diez. Ahora, necesitas crear otro valor DWORD bajo el nombre «MaxConnectionsPer1_0Server», dentro de la misma clave. De nuevo, asigna el número «10» (o el máximo de descargas que quieras permitir). Estos cambios se harán efectivos la próxima vez que reinicies el ordenador.

Ahorra tiempo con Explorer »

Navegar

Cuando llamamos a una dirección «.com», no es necesario que introduzcamos la dirección completa. Puedes ahorrarte el prefijo «www» y escribir solo el nombre del sitio, por ejemplo, «amazon» o «ebay». En lugar de presionar «Intro», presiona «Ctrl+Intro». Internet Explorer completará automáticamente la dirección. El atajo «Ctrl+D» añadirá automáticamente la página Web que estás viendo a tus Favoritos. Pero si quieres guardar el sitio en una carpeta específica de tus favoritos, es más rápido hacerlo de la siguiente manera: arrastra el icono de la dirección web (suele ser un icono de Internet Explorer, pero a veces está personalizado) desde la barra de direcciones hasta el menú de Favoritos y suéltalo en la carpeta que quieras.



Con un sencillo truco podrás deshacerte de Windows Messenger... y librarte de sus continuos intentos de conexión a Internet.

Suprime los módulos de Windows que no necesitas »

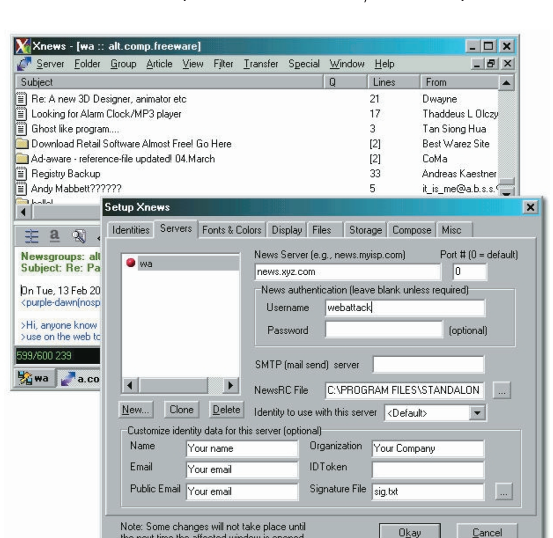
Windows Messenger

Windows XP instala algunas aplicaciones que no sólo ocupan espacio en el disco duro y en la memoria sino que provocan transferencias involuntarias de información: Windows Messenger es el mejor ejemplo. Para quitarlo de forma permanente, tendrás que editar un archivo del sistema llamado«sysoc.inf», que se encuentra en la subcarpeta Windows/inf. Abre el archivo con tu editor y busca la siguiente entrada: «msmsgs=msgrocm.dll, OcEntry,msmsgs.inf,hide,7». Borra la palabra «hide». Ahora, cierra y guarda el archivo. Abre el *Panel de control*, haz doble clic en *Añadir o quitar programas* y después en *Añadir/quitar componentes de Windows*. Ahora Windows Messenger aparecerá en la lista de componentes y podrá ser desinstalado.

Ahorra tiempo con los lectores de noticias »

Lectores Usenet

Usenet es una auténtica bola de nieve de información... Mayor cada minuto que pasa. Existe una gran cantidad de cosas útiles en ella, pero su tamaño hace que resulte difícil encontrar lo que se necesita. Tendrás que utilizar una herramienta especial que te permita curiosear y encontrar lo que buscas: un lector de noticias. Por supuesto, Outlook y Outlook Express, son programas muy bien diseñados para leer mensajes de texto, pero en lo que se refiere a otro tipo de archivos, como MP3, fotos o películas, no sirven para nada. Aquí te presentamos lectores especializados en archivos binarios, como Newsbin (**www.newsbin.com**, 27 euros) o News Rover (**www.newsrover.com**, 25 euros). Hacen listas de todos los servidores y grupos suscritos y manejan una cantidad casi ilimitada de conexiones, pero en un único servidor, por supuesto. Y son muy buenos guías en el laberinto. Xnews es gratuita. Esta herramienta ofrece una gran variedad de opciones y se puede descargar de la página **www.snapfiles.com/get/xnes.html**.



El lector de noticias gratuito Xnews proporciona una interfaz mucho más amigable para Usenet que la de las herramientas de Microsoft.

Consejos de hardware



NetGear WPN824

La nueva tecnología de NetGear, RangeMaxTM, elimina las zonas muertas y proporciona al usuario una conexión inalámbrica constante de alta velocidad, proporcionando una cobertura de 46.500 m2.
www.netgear.es

ASUS WL-500G Deluxe/WL-100G

Un router que puede también funcionar como puente inalámbrico entre las redes de comunicación de radio. Pero su velocidad no es mucho mayor que la del estándar «g». Proporciona dos puestos USB para discos duros externos, que son accesibles vía FTP y una webcam.
www.asus.com

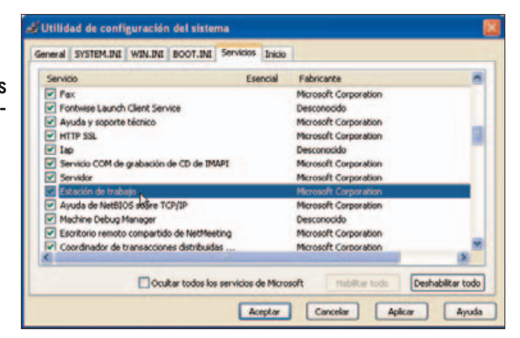
Mejor rendimiento en juegos en línea »

Turbo DSL

Los aceleradores prometen tiempos de descarga de páginas más cortos y mejor rendimiento para los juegos en línea. Y pretenden hacerlo habilitando la corrección del error algorítmico llamado *interleaving* o espaciamiento. El *interleaving* puede desaparecer porque el protocolo TCO/IP contiene ya un sistema de corrección de errores. Con el acelerador, la sincronización con la web y los servidores de juegos se acelera, reduciendo los tiempos de envío. Los jugadores en línea podrán disfrutar de esta ventaja al reducirse los tiempos de latencia. Algunos proveedores te harán pagar por ellos, pero otros lo incluyen en su servicio regular.



Los aceleradores reducen los tiempos de latencia en los juegos en línea.



Si descargas archivos de más de 100 Mbytes, puedes acelerar el proceso con gestores de velocidad como Reget.

Incrementa la velocidad con herramientas profesionales »

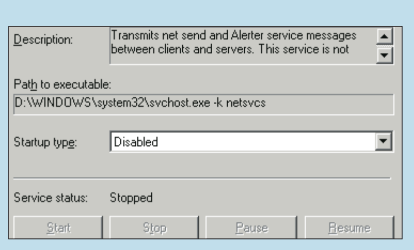
Ayuda para las descargas

Si elegiste DSL/WLAN para conseguir unas descargas más rápidas, deberías hacerte además con un cargador turbo. Especialmente para descargar películas o música. Prueba el software Reget (19 euros en **http://deluxe.reget.com/en/download.html**) durante 30 días antes de comprarlo. Reget consigue descargar ficheros en segmentos desde distintos servidores a la vez y recuperar descargas interrumpidas.

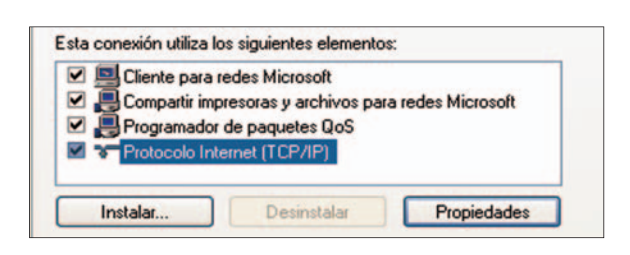
Cómo desactivar los servicios de mensajería »

Servicios Windows

Los servicios Windows no se circunscriben al PC, sino que establecen continuamente contacto con los servidores en línea de Microsoft. Puedes quitar de tu ordenador los siguientes servicios sin ningún problema: Messenger, Messaging, acceso remoto y telnet. Al hacerlo, estarás también desactivando algunas posibles fuentes de error. Para quitar los servicios del sistema, primero tienes que iniciar la Utilidad de configuración del sistema, escribiendo «msconfig.exe» en *Ejecutar* (accesible en *Inicio*). Después, haz clic en la pestaña de *Servicios*. Aparecerán todos los servicios del sistema. Haz doble clic en un servicio para abrir el cuadro de diálogo de *Propiedades*. Deshabilita y confirma la selección con *Aceptar*. Pero ten cuidado. Si deshabilitas algún servicios esencial por error, puedes paralizar todo el sistema. Este peligro no existe con el servicio Messenger. Es el responsable del intercambio de mensajes de alerta entre el cliente y el servidor (del todo irrelevante para los usuarios domésticos). Sucede lo mismo con el servicio NetMeeting Remote Desktop Sharing, telnet y TCP/IP NetBIOS Helper...proporcionan funciones que no necesitas en una red, intercambiando información entre los clientes asociados. Haz doble clic en los servicios innecesarios y después selecciona *Deshabilitado* como modo de inicio.



Desactiva servicios de sistema innecesarios; por ejemplo, Messenger.



Es posible acortar el tiempo de arranque a través de la configuración TCP/IP cuando el PC no esté conectado a una red local.

Arranques más rápidos con ADSL »

Dirección IP

La asignación de dirección IP propia no afecta sólo a las redes domésticas: los ordenadores independientes que utilizan una conexión a Internet se pueden beneficiar también de este pequeño truco. En los ADSL de usuarios independientes, el ordenador esperará en vano un servidor DHCP para asignar una dirección IP. Si ningún router DHCP o servidor está en funcionamiento, el fallo continuará hasta que se agote el tiempo. Para solucionarlo, quita la conexión TCP/IP de la red asociada al módem cuando instales el controlador PPPoE o, más sencillo, establece una dirección IP fija. Abre el Panel de control y haz clic en *Conexiones de red*. Introduce las propiedades de tu red inalámbrica, subraya *Protocolo Internet (TCP/IP)* y pincha en *Propiedades*. Introduce una dirección IP fija de clase C, como 192.168.1.1. A partir de ahora, el ordenador arrancará mucho más rápidamente.

Buscar servidores de noticias sin un lector »

Google

Es posible leer algunos grupos de noticias Internet Explorer. Los grupos de Google son un buen ejemplo. Son accesibles en la página de Google y conforman un centenar de grupos. Es una buena forma de comenzar a conocer cómo funciona el mundo de los grupos de noticias. Si utilizas servidores de noticias de forma esporádica, deberías buscar las ofertas gratuitas. Si lo que buscas es un servidor especializado en un tema, tendrás que buscar un poco más a fondo. Las búsquedas de Google como «nntp public news server» suelen dar resultados, pero sólo a veces. Otra forma es utilizar un servicio gratuito como Newzbot (**newzbot.com**). Esta herramienta ofrece una lista de servidores públicos y, entre otras cosas, muestra el número de grupos y la velocidad del servidor.

Los grupo de Google ofrecen chat y foros de distracción en todos los idiomas europeos.

Softwares, Downloads, Ebooks, Movies & Games
Group description: This group is all about Softwares, ebooks, Games, Movie
Category: Computers > Software
648 members, restricted

comp.sys.mac.system
Group description: Discussions of Macintosh system software.
Category: Computers > Systems
Usenet, public

n3td3v
Group description: Welcome. This security news wire is made of software de
incident response professionals, top thinkers and security aware peoples. Vi
Category: News > Breaking News
606 members

comp.cad.solidworks
Group description: SolidWorks newsgroup.
Category: Computers
Usenet, public

comp.sys.mac.apps
Group description: Discussions of Macintosh applications.
Category: Computers > Systems
Usenet, public

Los nuevos motores de noticias como NewzBot buscan en Internet servidores Usenet gratuitos que cubran los temas que más te interesen.


newzbot : search - group 'alt.binaries.sounds.mp3'

Found 4 servers that carry the newsgroup 'alt.binaries.sounds.mp3'
"Binary posting of mp3 sound files."
You can show all servers to display the one server that has no articles in the newsgroup 'alt.binaries.sounds.mp3'.

Server hostname	Articles	Days	Last post	Posting	Groups	Speed	Added	Verified	Comm
[illegible] (poor)	3248 (6K avg.)	398	26 days	Unverified	46495	56.20 K/sec	2001-01-12	1 hour	50
[illegible] (so-so)	2683 (252K avg.)	1	7 days	No	101076	55.69 K/sec	2003-01-10	8 days	3
204.153.244.171 (poor)	1658 (3K avg.)	30	14 days	No	32461	48.18 K/sec	2004-07-28	14 days	5



Belkin F5D8230de4/F5D8010de

Se trata de un router con un alto ratio de transferencia y con el alcance más grande de nuestro test. La aplicación para tarjeta PC sólo funciona con WEP. Registra un ratio de transferencia bajo con WPA cuando está encendido TKIP.
www.belkin.com

Gigabyte GN-B49G/GNWMAG

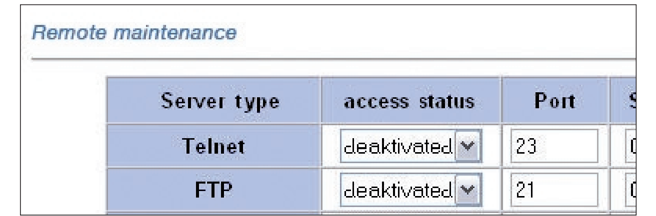
Un buen ratio de datos y una extraordinaria interfaz web. Ofrece una transmisión rápida y un gran alcance, pero su presentación podría mejorarse.
www.giga-byte.com





D-Link DWL-926

Se puede configurar fácilmente gracias a una buena interfaz web. El rendimiento es bueno, aunque la utilidad WLAN sólo puede utilizarse con WPA en la versión actual (3.1.6.31104).
www.dlink.com


Remote maintenance

Server type	access status	Port
Telnet	deaktivated	23
FTP	deaktivated	21

Desactiva el mantenimiento remoto (al menos por FTP y telnet) para que otros no puedan cambiar las configuraciones de tu router.

Protege tu router de accesos externos »

Mantenimiento remoto

Todos los routers comunes WLAN permiten mantenimiento remoto a través de Internet. Pero esta opción no siempre es segura, especialmente cuando el acceso se realiza a través de telnet o FTP. La configuración WLAN se hace normalmente de manera local; si quieres cambiar la configuración de forma remota, puedes dejar el acceso a la web abierto, pero tendrás que establecer una contraseña de seguridad.

Una nueva antena incrementa el alcance »

Antenas WLAN

Si la conexión entre el router y el PC es débil o se rompe con frecuencia, no siempre hay que culpar al adaptador WLAN de ello. Algunas veces, la potencia de transmisión y recepción son insuficientes. En este caso, deberías comprar una antena extra, con una potencia mayor que la que incluye la del router. El término técnico para medir la capacidad que una antena tiene de amplificar las señales entrantes en una dirección particular se llama «aumento direccional de antena» y se mide en dBi. Una antena incrementa significativamente el alcance tanto en las casas como en las oficinas.



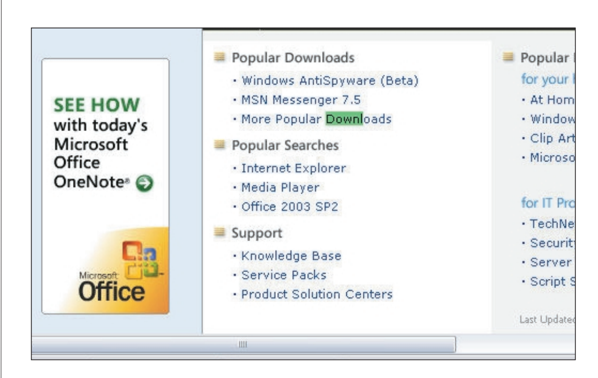
Cambia la contraseña »

Routers

El menú de configuración de red del router es accesible a través del navegador, escribiendo la dirección IP correspondiente. Encontrarás la dirección IP introduciendo «ipconfig» en Ejecutar, después de que se despliegue con el comando «cmd». De esta forma aparecerá la IP y la puerta de enlace estándar. Los menú de configuración de muchos routers son, por defecto, protegidos sólo por una contraseña estándar, como «Admin». Por esta razón, deberías asignar una nueva contraseña, más segura. Si no lo haces, las configuraciones del router podrán ser cambiadas por cualquiera. Deberías elegir una contraseña de al menos ocho caracteres, incluyendo números y caracteres especiales.



Sustituye la contraseña estándar por otra más segura.



Mozilla puede buscar un hiperenlace concreto, no importa lo intrincado de la página.

Oriéntate mejor en las páginas laberínticas »

Mozilla

La versión 1.6 de Mozilla te ayuda a navegar más rápido por páginas con cientos de hiperenlaces. Al presionar en el apóstrofe «'», Mozilla despliega la función «encontrar los enlaces tal y como se escriben». Después de eso, sólo tendrás que introducir las palabras de búsqueda. El navegador encontrará automáticamente el primer enlace que concuerde.

Sitecom WL-143

Además de cuatro puertos Ethernet, integra uno WAN. Cuenta con 15 puertos de acceso por direcciones MAC. En cuanto a seguridad, no incluye el cifrado 802.1x, una pena que acaba por estropear el resultado final del producto.

www.speed-2.com



Linksys WRT54G

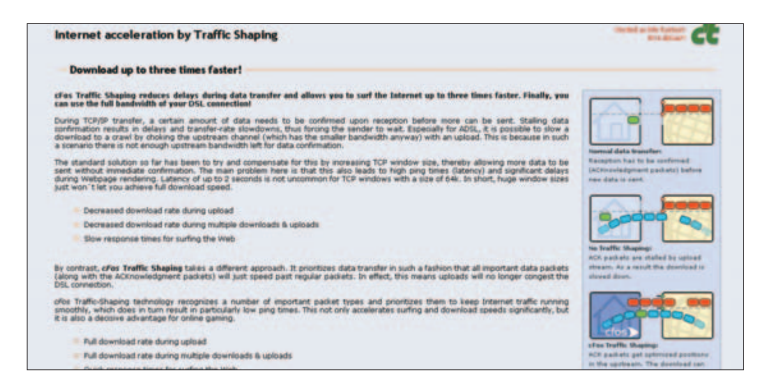
Estable en un entorno de interferencias, hay que asegurarse de actualizar el firmware para superar algún problema de seguridad de versiones previas. incorpora un sistema propio de transmisión.

www.linksys.

Límite de envíos »

Archivos compartidos

No solo el envío de mensajes con grandes archivos adjuntos puede retardar la velocidad de navegación: las herramientas que permiten compartir archivos también dan problemas. Esto se debe a una combinación de errores de TCP/IP y de la entrada de línea. La información se envía en paquetes. Cada uno de ellos debe ser confirmado por el que recibe con lo que se llama un informe ACK. Si se trata de un envío muy grande, el PC sólo puede enviar ACKs limitados al servidor si está funcionando con el programa de archivos compartidos, por lo que la descarga de páginas web se verá interrumpida. Para evitar que esto suceda, puedes limitar el volumen de envío en el software de archivos compartidos, lo suficiente para que los informes ACK no hagan más difícil la navegación. Puedes descargarte el controlador ADSL, Cfos, en www.cfos.de/oem por 28 euros. El truco de Cfos consiste en priorizar los paquetes pequeños de ACK en la lista de envío para que puedan enviarse más rápido.



El controlador Cfos acelera el tráfico de datos priorizando los paquetes más pequeños.

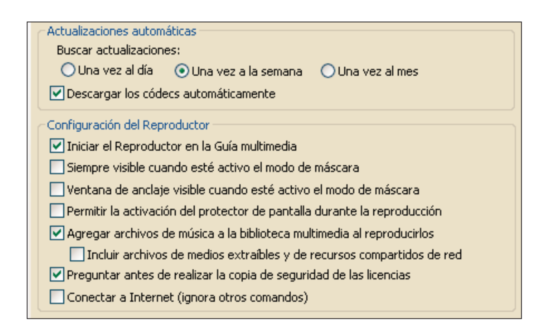
Limpia las cookies regularmente »

Control spyware

Los anunciantes se concentran en las informaciones personales, como las direcciones de correo electrónico y los hábitos de navegación. Algunos contenidos web generan *cookies* que envían información privada a un servidor central. Es lo que se llama gusano web, pequeños archivos gif escritos en CGI y que devuelven los datos al servidor original de forma dinámica. Los gusanos web no sólo se esconden en las páginas web, sino que pueden encontrarse en los correos electrónicos en formato HTML. Los programas antiespías como el gratuito Spybot Search o Destroy (**www.safer-networking.org**) y el servicio de privacidad en línea Pestscan (**www.pchell.com/pestscan**) te protegerán de estas invasiones. Internet Explorer guarda su gestor de *cookies* en *Herramientas/Opciones de Internet/Privacidad/ Avanzados*. Deberías deshacerte de ellas regularmente, sobre todo después de cada visita a páginas de descarga dudosa o páginas que contengan ofertas gratuitas... que suelen ser una señal de alarma.



El servicio en línea Pestscan ofrece control malware gratuito.



No dejes que Media Player siga conectándose sin avisar.

Prevenir la transferencia de datos indeseada »

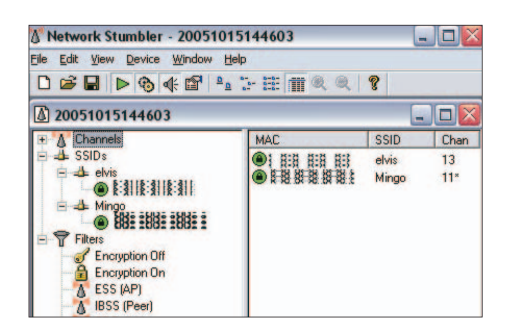
Media Player

Puedes quitar Media Player de la misma forma que quitaste Messenger. Porque Media Player busca actualizaciones de Internet sin que nadie se lo pida. Haz clic en *Opciones* del menú de *Herramientas* y cambia a la pestaña de *Reproducción*. Ahora desmarca la casilla *Descargar códecs automáticamente* y la de *Conectar a Internet*. Cambia a la pestaña de *Privacidad* para asegurarte de que ninguna opción está activada (excepto aquellas permitidas explícitamente por ti). En cualquier caso, te recomendamos que cambies de reproductor multimedia, por ejemplo, a uno como iTunes.

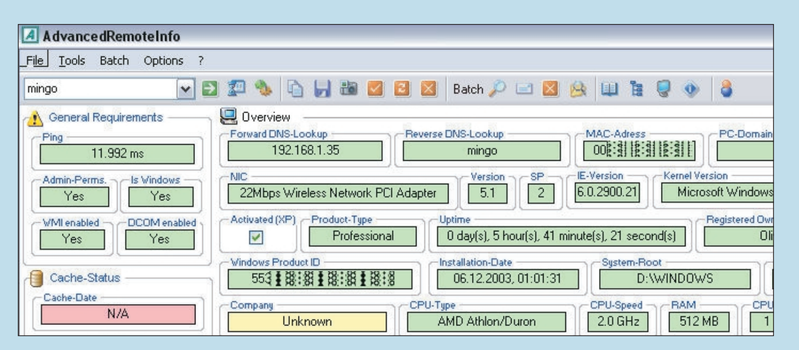
Con WLANs en competencia, cambiar de canal puede ser una ayuda »

Potencia de transmisión

Si tu vecino también tiene una WLAN, es posible que las dos redes se interfieran la una con la otra. Con Netstumbler (**www.netstumbler.com/downloads**) podrás averiguar fácilmente si las otras redes del vecindario transmiten desde el mismo canal que la tuya. Si es así, cambia la red a un canal libre para mejorar la calidad de recepción.



Si Windows reconoce más de una WLAN disponible, puede que haya interferencias entre ellas. Netstumbler busca si dos redes transmiten desde el mismo canal.



La herramienta AdvancedRemoteInfo despliega toda la información sobre IP y MAC así como la referente a dominio, hardware y sistema operativo.

Desarrolla una red rápida y un análisis del sistema »

AdvancedRemoteInfo

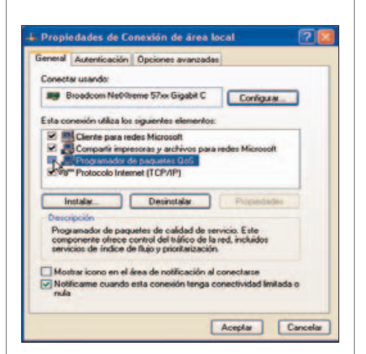
AdvancedRemoteInfo fue desarrollado originariamente para desplegar sistemas de información y diagnosis de errores dentro de las redes. Pero trabaja también muy bien en ordenadores independientes. Este pequeño programa escanea el sistema hasta encontrar todos los procesos y servicios en activo. Ayuda también a encontrar la dirección MAC, IP y el nombre del dominio con un solo clic de ratón. Además, esta herramienta informa sobre todo el hardware instalado y, en entornos cliente-servidor, informa sobre los usuarios registrados y sus derechos. Incluye un editor para enviar mensajes a otras cuentas de la red. Esta herramienta es gratuita y está disponible en **advancedremoteinfo.uptodown.com**.

Cómo acelerar nuestros datos al máximo

Aunque nuestra conexión a Internet sea rápida, es posible conseguir una velocidad mayor todavía. No sólo alcanzaremos esta velocidad al descargar archivos pesados, también al conectarnos a Internet e incluso en el envío de *e-mails*. El truco está en optimizar los valores de la tasa de transferencia en Windows.

1 Limitar el paquete QoS

Primero desactivamos el paquete QoS. Esta función de calidad de servicio es responsable de una corriente de datos constante y permanente en la red. Se trata de un servicio que demanda hasta el 20% del rendimiento de nuestro procesador. Los usuarios de Windows XP Profesional pueden desactivarlo completamente, mientras que los usuarios de la versión doméstica del sistema operativo no cuentan con este servicio. Antes que nada, quitamos la marca de la opción *Programador de paquetes QoS* en el *Panel de control/Conexiones de red/Propiedades de conexión de área local* y a continuación presionamos el botón *Desinstalar*. Utilizamos *Inicio/Ejecutar* e introducimos *gpedit.msc* por lo que conseguimos la política de grupo. En la columna izquierda navegamos hasta *Configuración del equipo/Plantillas administrativas/Red* y a continuación vamos a la entrada de *Programador de paquetes QoS*. Hacemos doble clic sobre la entrada *Limitar ancho de banda reservado* en la columna derecha. En la caja de diálogo *Propiedades* accedemos a la preconfiguración. Esta acción es únicamente necesaria si vemos *Habilitada* en el área superior y si el valor *20* se muestra en la ventana desplegable junto a *Límite de ancho de banda*. En ese caso reducimos el valor a un número entre 1 y 5. Si experimentamos algún tipo de problemas mientras avanzamos en el procedimiento, deshacemos el paso completo o incrementamos el valor de QoS.



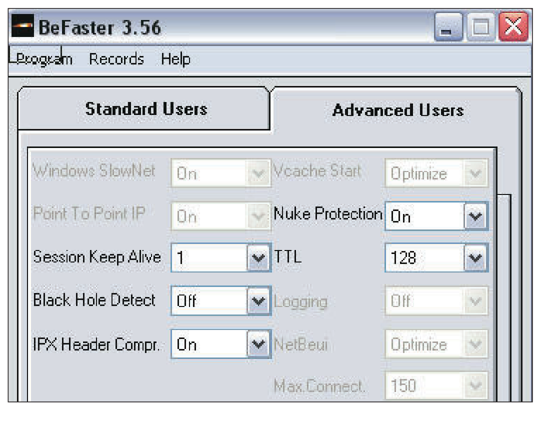
1 Si se activa el servicio *QoS*, sólo reducimos el ancho de banda reservado o lo desactivamos totalmente.

2 Una vida más larga para los datos

Las configuraciones de red falsas suponen la no transmisión de algunos de los datos al receptor, por lo que no visualizarán ninguna página web o bien se mostrarán con errores. Esto es debido al valor TTL que dicta los segundos que un paquete tarda en ser rechazado. El valor estándar es 32, de modo que cada *router* que envía un paquete de datos resta 1 a ese valor. Si alcanza el número cero, será rechazado. Configuramos un valor TTL más alto posible para así evitar un rechazo prematuro de los datos. Para configurar este valor, podemos utilizar Befaster (**www.shareup.com/BeFaster-download-1223.html**). Debemos evitar incrementar este valor si no es imprescindible: 128 segundos es una buena opción. Un *site* puede no abrirse por una serie de razones técnicas, por lo que es aconsejable medir los tiempos muertos antes de configurar el valor.

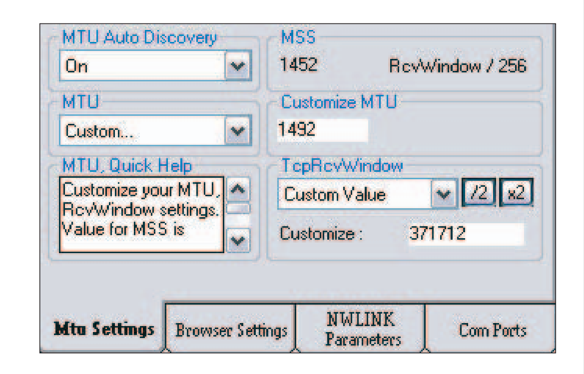
3 Configuración óptima

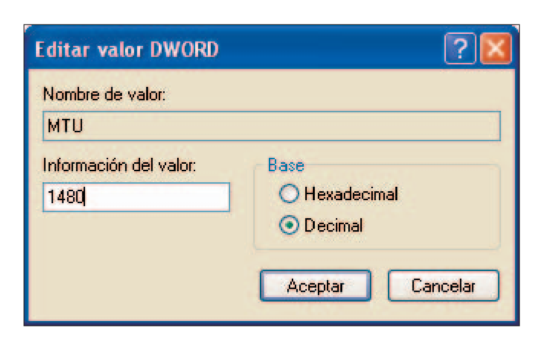
Un valor MTU falso puede ser el responsable de una conexión fallida. El valor más alto configurado es de 1.500 Bytes. Muchas veces se piensa que con el valor más pequeño tendremos una caída importante en el rendimiento, una teoría que no es del todo cierta. Con la ejecución de los valores más altos ponemos en peligro la transferencia de datos, ya que los paquetes trabajan en el modo fragmentado por lo que el servidor tiene que reunirlos. Comprobamos lo comentado con el comando *ping*. Abrimos la opción *Ejecutar* desde el menú *Inicio* y tecleamos *cmd* y a continuación *ping* con el parámetro *–f –l* y el valor *1500*. Agregamos un espacio y cualquier dirección web. Si estamos conectados a Internet, nuestro ordenador enviará paquetes de este tamaño al servidor relevante. Repetimos esta acción con valores más pequeños hasta conseguir el



2 Cuando experimentamos pérdida de datos durante la transmisión, resolvemos el problema incrementando el valor TTL.

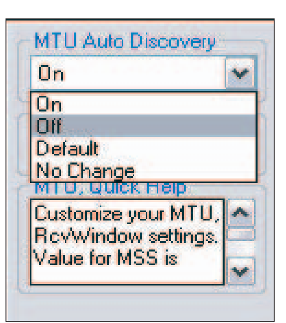
3 Con los valores MTU optimizados, los datos se enviarán a través de paquetes más pequeños.



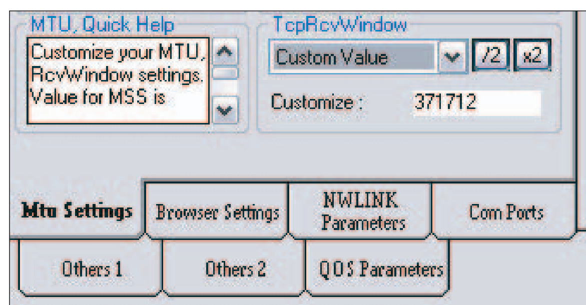



También en el Registro, podremos establecer el valor MTU para cada dirección IP.

5 La función ***MTU Auto Discovery*** puede desactivarse, si hemos encontrado el valor MTU óptimo.



6 Podemos determinar los datos a través del valor RWIN en el valor MTU.



valor óptimo. El baremo debería estar entre 460 y 1492. Para configurar el valor MTU permanentemente, utilizamos Befaster (**http://www.shareup.com/BeFaster-download-1223.htm**).

4 Editar los valores MTU en el Registro

Para comprobar los valores antiguos o para ejecutar manualmente los cambios en tu sistema o en otros, tienes que configurar un valor de registro. Primero necesitas tu propia dirección IP. Esto es sencillo. Haz clic con el botón derecho del ratón sobre el símbolo de red (*Panel de control/Conexiones de red*) y selecciona *Estado*. En la pestaña *Soporte* encontrarás el número. Para abrir el Editor del Registro ve a *Inicio/Ejecutar* y escribe regedit. Ve a la clave *HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlerSet\Services\Tcpip\Parameters\Interfaces*. Escoge la carpeta con tu propia dirección IP o la proporcionada por el servidor (DhcpIPAdress). Haz clic en una zona vacía de la ventana de la derecha con el botón derecho del ratón y, del menú contextual, escoge las opciones *Nuevo/Valor DWORD*. Etiqueta el nuevo valor con MTU. Haz doble clic en la nueva entrada. En la ventana de edición, marca la base *Decimal* y rellena la *Información de valor* de forma óptima (en este ejemplo, «1480»). Presiona *Aceptar,* cierra el editor y reinicia.

5 Sin prueba y error

Si te estás comunicanco con un servidor en el otro extremo del mundo, el flujo de datos se ajustará a la velocidad del servidor más lento de la cadena: esto se aplica especialmente a los valores MTU. No importa cuántos bytes hayas indicado en el Registro, el tamaño máximo del paquete depende de la respuesta del servidor si éste proporciona un valor menor. Windows realiza automáticamente la negociación del tamaño de los paquetes, y se toma su tiempo en ello. Si has encontrado el valor óptimo para tu conexión, puedes desactivar esta fución con Befaster. Lo peor que puede pasar es que los paquetes sean fragmentados y que se ralentice la operación de Windows.

6 Procesamiento de datos RWIN

Mayor procesamiento de datos no significa necesariamente mayor velocidad, aunque ambos estén relacionados. La configuración de Windows RWIN determina cuántos datos pueden ser recibidos sin que tengan que enviar confirmación. Es por ello que el valor RWIN debe ser varias veces mayor que la cantidad de datos que puede ser enviada en un bloque de datos. De otra forma, la descarga de *streaming*, por ejemplo, se verá constantemente interrumpida. Verás que la velocidad no aumenta si cambias el valor aleatoriamente. Los datos se perderían en la transferencia, pues la confirmación necesaria se habría perdido o llegaría demasiado tarde. El valor RWIN apropiado depende directamente del valor MTU y se calcula como sigue: MTU menos 40, multiplicado por 4. Así, un valor MTU 1492 supone un número RWIN 5808. Configurar este valor así nos proporcionará una navegación más suave y sin interrupciones. Para comprobarlo, intenta multiplicarlo por 8 o incluso 16. Puedes fijar el valor RWIN con una herramienta shareware como Befaster.

GLOSARIO

QOS: Quality of Service **(calidad de servicio) es un término técnico de tráfico de datos que se refiere a la probabilidad de que un paquete logra viajar entre dos puntos de la red.**

TTL *TIME TO LIVE* (tiempo de vida) es el límite del periodo de tiempo durante el cual un paquete de datos puede existir antes de ser descartado. El valor TTL se encuentra en la cabecera de la IP y está indicado por el remitente. Es reducido por cada Host que encuentra hasta su destino. Si se termina, el paquete es descartado y le llega un error al remitente (*Time Exceeded*). Esto evita situaciones en las que un paquete que no se puede entregar siga circulando por la Red.

MTU *Maximum Transmission Unit* (unidad máxima de transmisión) es un término que se da al tamaño (en bytes) del paquete mayor tamaño enviado por un protocolo de comunicación como IP. Los datos enviados vía IP son fragmentadas en pequeñas piezas por el remitente. El receptor las vuelve a ensamblar para convertirlas en los datos originales.

RWIN El receptor TCP de Windows describe la cantidad de datos que el ordenador puede tolerar sin comunicárselo al remitente. Si no es reconocido el primer paquete, el remitente, el envío se detendrá y esperará y, si pasa cierto tiempo, vuelve a enviar el paquete de nuevo.

Preguntas y respuestas

Cuando hay un atasco en la autopista WLAN, no necesariamente es culpa de tu router. Otras redes WLAN pueden interferir, o tu proveedor de Internet podría tener problemas técnicos.



Los routers MIMO como éste de Belkin tienen más de dos antenas, controladas por un procesador de señales, lo que proporciona un flujo de datos constante.

Si la velocidad de tu conexión WLAN ha descendido notablemente, tienes que enfocar el problema metódicamente. Primero comprueba si la conexión es estable o si hay datos cargándose de fondo. Quizá la respuesta del servidor está ralentizando la transferencia de datos. Para comprobar el tráfico de datos de cierto servidor, puedes utilizar el comando tracert desde el símbolo de sistema.

? ¿Qué es una WLAN ad hoc?

! Una WLAN *ad hoc* es una conexión directa entre dos ordenadores sin un router. Esto significa que los PCs pueden compartir rápidamente sus datos. Tener más de dos PCs conectados tiene sentido si , por ejemplo, quieres jugar en red. Para acceder a la red actual o a una estructura de red ya instalada, necesitas un punto de acceso.

? Tengo una WLAN y quiero integrar dos PCs más. ¿Tengo que actualizar mi hardware?

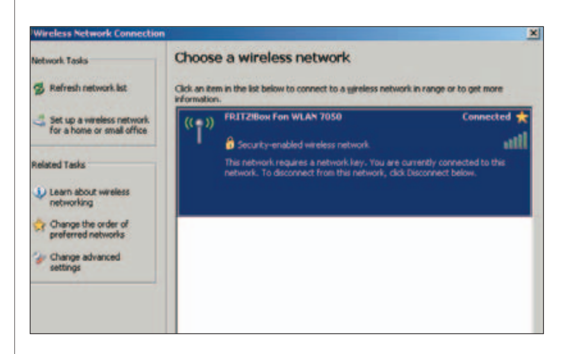
! No siempre. Si todos los PCs tienen adaptadores WLAN, inténtalo sin actualizar. Teóricamente, un punto de acceso puede ser útil para 255 clientes diferentes, aunque en la práctica las cosas no son tan sencillas. Por regla general, con un ancho de banda de 11 Mb/s, de diez a quince clientes pueden compartir una conexión, mientras ninguno de ellos se esté bajando grandes cantidades de datos. Lo más importante es que los clientes estén lo más cerca posible del punto de acceso y que el flujo de datos sea estable.

? ¿Qué ventajas supone el nuevo estándar MIMO?

! MIMO (*Multiple Input Multiple Output*) es un modo totalmente nuevo de hacer WLAN que casi dobla las actuales tasas de transferencia. MIMO utiliza una serie de antenas para lograr la mayor potencia de envío al router. No todas las antenas tienen siempre la misma fuerza de señal, pues el procesador de señales produce múltiples vías de señal. Esta división de la carga es crucial, permitiendo que la calidad de la conexión sea estable. Algo muy importante para procesos sensibles al tiempo como el *streaming*. Ya hay routers a la venta con tecnología MIMO. Puedes reconocerlos por las tres o más antenas que incorporan.

? La velocidad de mi conexión WLAN desciende cada tarde a la misma hora. ¿Por qué motivo?

! Hay muchas posibles causas. La más habitual es que el tráfico de datos en la red aumenta por las actualizaciones diarias (quizá se ejecuten automáticamente de fondo). Quizá otros usuarios de la red utilicen un ancho de banda mayor a esa hora, aunque eso sólo sería un problema si hubiera tres o más personas navegando y cargando datos a la vez. Primero comprueba si la calidad de tu conexión es buena. A veces muchas WLAN se bloquean unas a otras si están activas al mismo tiempo. Desconecta tu conexión de red y cambia el canal utilizado por tu router. Vuelve a conectar y comprueba su calidad.



Si múltiples WLAN se bloquean, el ancho de banda desciende. En esta situación cambia el canal por defecto del router. Un posible problema es que Windows reconozca múltiples WLAN con amplios rangos de señal.

? ¿Puedo aumentar el radio de alcance utilizando más de un punto de acceso?

! Buena idea. Según el número de usuarios conectados de forma inalámbrica, puedes emplear hasta 13 puntos de acceso (el número máximo de canales diferentes disponible en Europa) en un entorno inalámbrico grande. Los puntos de acceso tienen que utilizar diferentes canales en el rango de frecuencias compartido. El alcance disponible y el ancho de banda total aumentarán.

PONTE AL DÍA

La popularidad de Windows XP se debe sobre todo a que ha conseguido integrar de manera sencilla y amena recursos de red y características multimedia. Posee una gran cantidad de funciones que hacen que su utilización sea más sencilla...Sigue leyendo y tu vida informática será mucho más simple y gratificante.





Configurar una red es más fácil de lo que imaginas

Si eres nuevo en la red, puede parecerte complicada. Por suerte, Windows XP incluye una gran cantidad de funciones que te permitirán conectar tus ordenadores al gran mundo.

Existen muchas razones por las que deberías pensar en configurar una red doméstica. Es un error creer que esto es algo que sólo conviene a las empresas. Básicamente, una red es la manera más rápida de transmitir información y sólo podrás vivir sin una si eres de los que prefiere copiar CDs y llevarlos por toda la casa. Porque, por supuesto, es mucho más conveniente arrastrar los archivos hasta el disco del otro ordenador que escribirlos y luego copiarlos en un DVD. En una red, es facilísimo hacer copias de seguridad de tus datos copiándolos en otra máquina. En un ordenador independiente, tienes que ser muy disciplinado y copiar tus archivos día a día. Otra ventaja es la opción de compartir recursos. Sale más barato comprar una impresora y que pueda utilizarla toda la familia, que tener una para cada ordenador de la casa. Existe otro recurso importante que puede compartirse: tu conexión a Internet de banda ancha. Cada vez más hogares utilizan una conexión de banda ancha como ADSL o cable. Un router es una excelente manera de minimizar costes y rentabilizar tu suscripción al máximo.

DE ACUERDO, CONFIGURAR UNA RED WINDOWS constituye un desafío si no lo has hecho nunca antes. Pero, afortunadamente, incluso los principiantes pueden llegar a hacerlo si tienen en cuenta algunas cuestiones básicas.

En primer lugar, la planificación es fundamental. Decide la cantidad de procesamiento que necesitas, establece si quieres WiFi o Ethernet (o cualquier otro tipo exótico de red como PLC, que se enchufa en la toma de corriente). Averigua qué dispositivos tienes ya disponibles, porque muchos ordenadores integran ya Ethernet y Wifi. Compra todo el equipo que necesites, lee el libro de instrucciones, instala las tarjetas de expansión necesarias y sus controladores. Ni siquiera pienses en configurar la red antes de instalar el hardware necesario.

Windows XP ofrece ICS (*Internet Connection Sharing*), una función que permite a una máquina XP compartir su conexión Internet con otros ordenadores de la red. Por consiguiente, no necesitas



Instalar una red es la mejor manera de establecer «colaboración» entre distintos sistemas, como Mac y Windows XP.

“XP te ofrece una amplia gama de servicios”

utilizar un router de banda ancha si no quieres. Sin embargo, creemos que es mejor utilizar uno, porque verdaderamente facilita la configuración y el uso de la red.

PUEDES ESCOGER ENTRE DOS FORMAS. En primer lugar, puedes optar por hacerlo todo automáticamente. En este caso, compra un router, conecta todos los ordenadores a él y haz funcionar el asistente de red de cada máquina. De esta forma, todo debería ir como la seda. En segundo lugar, puedes asignar la dirección IP manualmente. Aunque es mucho más trabajoso en un principio, a la larga es una fórmula mucho más sencilla porque te libra de problemas posteriores.

Si pretendes compartir archivos con XP Home, verás que las funciones son muy básicas. XP Home sólo ofrece el sistema sencillo (*Simple File Sharing*), que no permite configurar permisos para cada uno de los usuarios. Esto significa que, o compartes los archivos con todos los ordenadores de la red, o no podrás compartirlos con nadie. La única cosa que puedes hacer es esconder un compartido de manera que la gente que no sepa de su existencia no se dedique a buscarlo. A diferencia de las antiguas versiones de Windows, Windows 98 o Millenium, Windows XP Home ni siquiera ofrece la opción de proteger un compartido con una contraseña. Aunque hay quien da «consejos» para saltarse estas limitaciones, lo cierto es que son difíciles de superar.

CON WINDOWS XP PROFESIONAL puedes optar o por *Simple File Sharing* o por la función que ofrece un completo sistema de permisos (que quizá conocerás por el mundo empresarial). Normalmente, en una red familiar no tendrás necesidad de establecer permisos para cada usuario, por lo que será mejor que elijas el sistema sencillo. Pero si lo que vas a montar es una pequeña oficina, entonces hay varias cosas que necesitas saber. Para instalar una red empresarial necesitas Windows XP Profesional (o un servidor Samba, algo que por el momento se sale de los objetivos de este artículo). Para establecer los permisos, ten en cuenta que se aplicará siempre el nivel de permisos más restrictivo para tus compartidos y para tus NTFS, por lo que si detectas algún problema, verifica siempre los dos tipos.

Una vez configurado, operar y detectar problemas es mucho más fácil si tienes algunos conocimientos básicos sobre las propiedades internas. Sigue leyendo para adquirir algunas nociones básicas.

TODOS LOS ORDENADORES EN INTERNET, así como los que se encuentran en una red privada, necesitan un número único, el llamado número IP. Comprende cuatro bloques, llamados octetos, y se parecen a: «192.168.123.254». La primera razón para que una red no funcione es que se haya perdido el número o se haya asignado uno que no es correcto. Un ordenador puede obtener su IP de dos formas: dejando que le sea asignada por una función de los routers de banda ancha llamada DHCP, o asignándoselo manualmente. Si se hace de forma manual, no se puede elegir cualquier número. Debe ser parte de la misma subnet de la dirección IP de tu router, debe estar entre 0 y 25, y tiene que ser único. Por tanto, si utilizas un ordenador XP con ICS como router, su IP será 192.168.0.1: tu subnet es, por consiguiente, 192.168.0.x, y puedes asignar también algo como 192.168.0.2. Si utilizas un router de banda ancha externo, debes leer su libro de instrucciones para saber qué IP utiliza.

Cuando los PCs tienen números IP en la misma subnet, pueden comunicarse entre ellos. Por supuesto, «comunicarse» y «compartir archivos» son cosas muy diferentes. Así, después de asignar una IP, podrás utilizar la conexión compartida a Internet desde cualquier ordenador, pero los ordenadores no podrán tener acceso a las carpetas de los demás. El proceso de hacer los archivos accesibles a los demás ordenadores se llama «compartir».

Trucos para establecer permisos con Windows XP

1) Recuerda que *Todos* (un sistema de grupo en el que todos y cada uno de los usuarios es un miembro) tendrán automáticamente permiso para leer cada archivo compartido que se cree. Cambia esto si quieres mantener un compartido en privado.

2) Para hacerlo, elimina la entrada *Todos*. No deniegues el permiso a *Todos*. Si lo haces, también te lo estarás denegando a ti.

3) Los permisos son inherentes a los distintos grupos de los que eres miembro. Si te pierdes, hay una herramienta que muestra los permisos válidos. Haz clic en el botón derecho del ratón sobre la carpeta, elige *Propiedades*, pincha en *Seguridad* y después *Extender*. Haz clic en la pestaña de *Autorizaciones efectivas*, elige el usuario o grupo y consulta los permisos en vigor.

4) Los permisos de los NTFS pueden cambiar cuando mueves los archivos y las carpetas. Depende de si la carpeta de llegada está en el mismo volumen NTFS o no y de si «Mueves» o «Copias». Si tienes dudas, deberías revisar el estado en la pestaña de *Seguridad* después de copiar.



Consigue una intalación de red adecuada antes de empezar

Megabit, hubs, switches... palabras que pertenecen a la jerga de los expertos de redes. No tienes por qué ser un especialista para administrar tu propia WLAN.

Antes de comprar »

Hardware

Tenemos varios ordenadores y queremos construir una red. Antes de comprar el hardware, comprueba si las máquinas tienen integradas los *plug-ins* de red (los más nuevos si lo hacen) y si soportan FastEthernet (100 Mbps) o Gigabit Ethernet (1.000 Mbps). Si alguno o todos estos equipos soportan, únicamente, FastEthernet, queda en tu mano decidir si te gastarás un poco más de dinero en tarjetas Gigabit Ethernet. También necesitarás un *switch* o conmutador. Si optas por un equipamiento Gigabit, asegúrate que consigues un modelo sin ventilador (los *switches* FastEthernet nunca lo incorporarán).
Los *switches* Gigabit Ethernet sin disipador trabajan bien y son más silenciosos. Un router de banda ancha tiene dos características: hace que tu conexión a Internet esté disponible para todos los clientes de una red y, dado que integra un firewall, tu red quedará protegida. Este tipo de *routers* suelen ofrecer muy pocos puertos Gigabit.





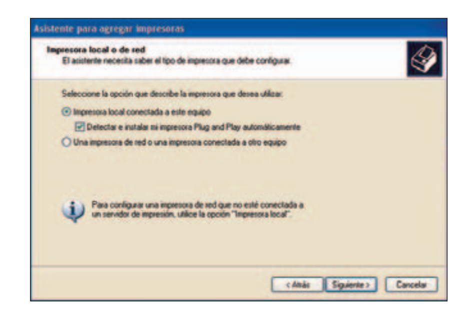
Decidir un emplazamiento »

Infraestructura de la red

Antes de nada, conviene trazar un dibujo de tu red. Decide si quieres una red Wi-Fi (es muy sencilla de instalar) o una Ethernet (más rápida, económica y segura, pero con cables de por medio). Incluso, podrías optar por una red mixta que combine cosas de ambas. ¿Cómo actúan las redes de hoy en día? Cada ordenador se conecta directamente a un *switch* principal (excepto cuando introduces *switches* adicionales como *hubs* secundarios). Por este motivo, piensa detenidamente dónde quieres colocar el *switch* principal. Si tu conexión telefónica está mal situada, podría merecer la pena extender el cable del teléfono. Es preferible ubicar la impresora en red en un punto que sea accesible para todos.

Imprimir desde XP »

Impresoras en red



Si tienes una red doméstica y una impresora con un *plug-in* de red integrado podrás acceder desde cualquier ordenador de tu red. Encuentra su dirección IP en el correspondiente manual. Cambia esta IP a una dirección que se encuentre dentro de tu rango IP. Haz clic en *Inicio* y dentro del *Panel de control* escoge la opción *Impresoras y faxes*. Sigue la ruta *Archivo/Agregar impresora*. De las opciones que, a continuación, tendremos en pantalla deberemos escoger *Impresora local conectada a este equipo*. Nos aseguramos que deshabilitamos la casilla *Detectar e instalar mi impresora Plug and Play automáticamente* y pulsamos *Siguiente*. Ahora, escogemos la opción *Crear nuevo puerto* y especificamos el tipo de puerto, que en este caso será *Estándar TCP/IP*. Haz clic más de dos veces. Introduce la IP de tu impresora y confirma. Te preguntará por los *drivers* de ésta, que están en el CD del fabricante.

Impresora compartida »

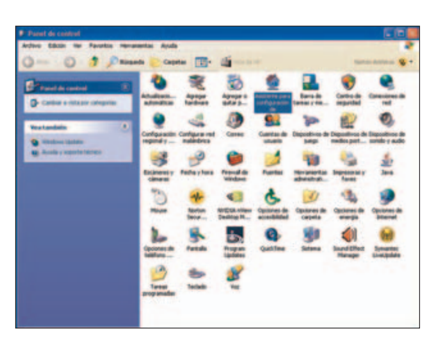
Herramientas DOS

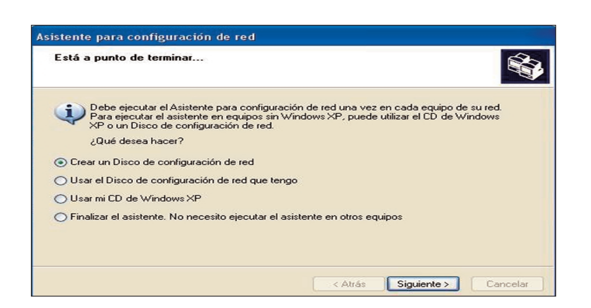
Una herramienta DOS podría impedir la posibilidad de imprimir en una impresora compartida, demandando en su lugar una de tipo local LPT1. Existe una manera para hacerle creer que una impresora compartida se encuentra conectada de forma local. Dentro de *Inicio*, dirígete a *Ejecutar*. Introduce *CMD* y presiona la tecla «Intro». Con cuidado, escribe: *net use lpt1:\\<print server>\<shared printer> /persistent:yes*. Reemplaza <print sever> y <shared printer> por los nombres correctos de tu sistema. Pulsa «Intro».

Instalación sencilla »

Asistentes

Microsoft incluye en Windows XP un Asistente que nos ayudará a montarnos nuestra red. Primero instalaremos las tarjetas de red con sus respectivos *drivers* para, posteriormente, conectarlos a un *switch* o router.
En el primer PC, seguiremos la ruta *Inicio/Panel de control/Asistente para configuración de red*. Pulsa sobre el botón *Siguiente* en las dos siguientes ventanas. A continuación, especifica si tu PC tiene una conexión directa a Internet (si no tienes un router de banda ancha) o si lo hace a través de un *gateway* o pasarela. En la siguiente ventana escogeremos una palabra que describa nuestro equipo (fácilmente identificable) y otra para especificar el nombre de éste. Date cuenta que necesitaremos el mismo nombre para los otros ordenadores. Si seguimos las indicaciones del Asistente, ahora activaríamos el uso compartido de archivos e impresoras.

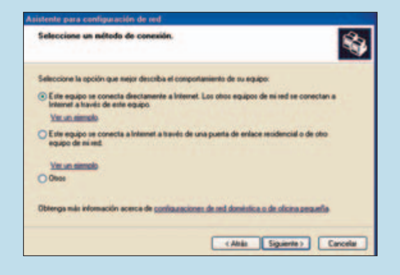




Integrando antiguos PCs con Windows »

Configurar un disquete

XP fue el primer sistema operativo de Windows que incluyó un Asistente de instalaciones de red. La integración de antiguos equipos podría, hasta la fecha, desalentarnos si no éramos unos expertos en el tema de redes. Cuando ejecutas el instalador de redes de la mano de XP, al final del proceso te encontrarás con la opción de crear un disquete. Éste albergará un único archivo que será requerido para ejecutar un ordenador que no tenga instalado Windows XP. Esto nos va a permitir configurar una red con todas las facilidades que el Asistente de este sistema operativo nos brinda.



Compartir la conexión a Internet »

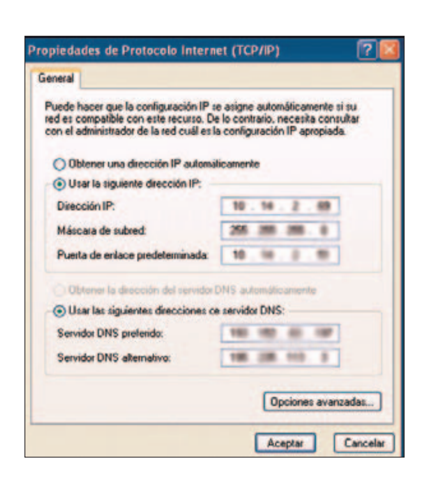
Sustitución del router

Windows XP tiene lo que se conoce como ICS (Internet Connection Sharing), que nos permite utilizar un ordenador con Windows XP como un router. Es muy fácil de utilizarlo. Ponemos en marcha el Asistente para configuración en red y escogemos la opción *Este equipo se conecta directamente a Internet*. En la pantalla que permite determinar la opción que mejor describe cuál es el comportamiento de nuestro equipo, escogeremos nuestra red. Si creas un disco de configuración de red al final, tus clientes de se configurarán correctamente manera automática. Utilizando los ICS, tu servidor (el PC con la conexión) tendrá una IP estática (por ejemplo 192.168.0.1). El resto de las cajas obtendrán números pertenecientes al mismo rango. Con un buen router gastarás menos electricidad y generarás menor ruido, y dispondrás de un firewall más seguro que el de Windows, además de contar con acceso compartido a Intenet.

Asignando números »

Numeros IP

Cada ordenador en una red IP tiene una única dirección que le sirve como medio de identificación. Puedes permitir a tu router de banda ancha asignar estos números IP automáticamente. De todas maneras si, por ejemplo, vas a cambiar tu red en un futuro, es preferible asignar direcciones IP manualmente. Para ello, lo primero es localizar la dirección IP de tu router de banda ancha (búscalo en su manual). Ésta debería ser similar al ejemplo que aquí te mostramos: 192.168.123.254. Consigue una hoja de papel, toma nota de todos tus ordenadores y escribe sus direcciones IP al lado de ellos. Aunque puedes utilizar cualquier número, en el caso del último bloque éste se encontrará entre el 0 y el 255 (procura que sean diferentes). En cada PC, sigue la ruta *Inicio/Panel de control/Conexiones de red*. Abre las propiedades de tu conexión LAN, haz un doble clic en *Protocolo Internet (TCP/IP)* y escoge *Usar la siguiente dirección IP*. Ahora incluye tu dirección IP. Introduce, por ejemplo, 255.255.255.0 como *Máscara de subred* y tu router IP como *Puerta de enlace predeterminada*, así como *Servidor DNS preferido*. Pulsa *Aceptar* dos veces.





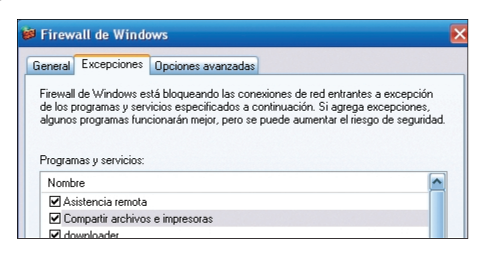
Archivos y carpetas disponibles para toda la familia

Ten cuidado. La mayor parte de los problemas de una red residen en una configuración errónea de compartición. Toma nota de los siguientes consejos.

Configurando tu firewall »

Bloqueo

Los firewall se crearon para proteger a nuestro ordenador de posibles ataques externos. Resulta obvio que compartir archivos entraña riesgos. Por esta razón, la mayoría de los firewalls incluyen una opción que restringe el compartir archivos. Dado que podemos pasarnos horas y horas solucionando los problemas derivados de compartir archivos que no funcionan, conviene comprobar las características de nuestro cortafuegos. Si tienes Windows Firewall, dirígete a *Inicio*. Dentro del *Panel de control* haz un doble clic en *Windows Firewall* y pulsa la pestaña *Excepciones*. Asegúrate que la opción *Compartir archivos e impresoras* está activada.



Uso compartido simple de archivos »

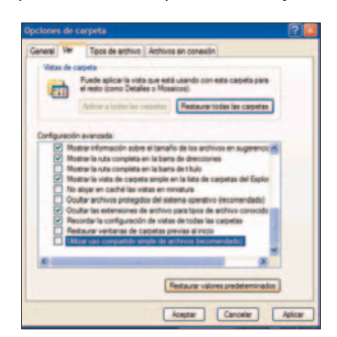
Compartiendo

Vamos a disponernos a compartir. En la pestaña *Compartir*, en la sección *Uso compartido y seguridad de red* marca el campo *Compartir esta carpeta en la red*. Esto no resulta obligatorio desde que Windows usa el nombre de la carpeta si dejas el nombre del campo en blanco. Para que la compatibilidad sea máxima, utiliza nombres de más de 8 caracteres. Si tu red únicamente trabaja con XP, olvida las restricciones y emplea nombres compartidos con cualquier longitud o extensión. Si marcas la opción *Compartir esta carpeta en la red*, cualquiera que pertenezca a tu red podría modificar o suprimir los archivos localizados en la zona que compartes. Pero si no lo marcas, los usuarios de la red únicamente accederán a la lectura de su contenido, pudiendo abrir cualquier archivo pero no modificarlo o eliminarlo.

Desactivar el uso compartido »

Permisos

Si utilizas la versión doméstica de XP, debes saber que ésta soporta la característica de compartir archivos simples, algo que no nos obligará a configurar distintos permisos para varios usuarios. Con la versión profesional es diferente, ¿el motivo? Que automáticamente desactiva esta opción en un entorno de empresa (cuando la máquina se une a un dominio). Utilizando la versión profesional de XP y si quieres configurar los permisos dentro de un grupo, tendrás que desactivar dicha característica manualmente. En *Inicio*, dirígete a *Panel de control*. Haz doble clic en *Opciones de carpeta*. Marca la pestaña *Ver* y desactiva la caja *Utilizar uso compartido simple de archivos (recomendado)*. Haz clic en *Aceptar*. Ahora, ya estás en condiciones de utilizar permisos explícitos. Por supuesto, los que tengan la versión doméstica de XP (Home Edition), no dispondrán de la opción que hemos explicado.



Funciones ocultas »

Archivos secretos

Las partes cuyos nombren acaban con un signo del dólar no aparecerán en el resto de los ordenadores de la red. Esto resulta cierto, incluso, en los equipos con una versión doméstica de XP. Además, esta es la única manera que existe de distinguir a los usuarios individuales que ejecutan este sistema operativo. Imagina que quieres que tu hermano acceda a una parte, pero no tus padres. Crea una parte con un nombre que acabe en $, como por ejemplo *especial$* y hazle saber a tu hermano que ese va a ser su nombre. De esta manera, él accederá a ésta tecleando en la dirección de Windows el campo *el nombre de tu PC o dirección IP>\especial$*.



Compartiendo la primera vez »

Falsa alarma



Tanto si tienes la versión doméstica como profesional de XP con sus configuraciones por defecto, la posibilidad de compartir archivos resultará sencilla. Haz clic con el botón derecho del ratón en la carpeta que quieres compartir y escoge la pestaña *Compartir y seguridad*. La primera vez que hagas esto, apreciarás un mensaje que te indicará que la opción de compartir está desactivada en el ordenador. Llegados a este punto puedes utilizar, si lo crees necesario, la ayuda que te facilita el Asistente. Ignora esta advertencia, haz clic en la opción *Usar el asistente para habilitar uso compartido de archivos (recomendado)* y luego en *Aceptar*. La utilización del Asistente no ofrece ninguna ventaja. La única diferencia es que comparte la carpeta de Documentos Compartidos sin comunicártelo.

Compartir archivos a través de Internet »

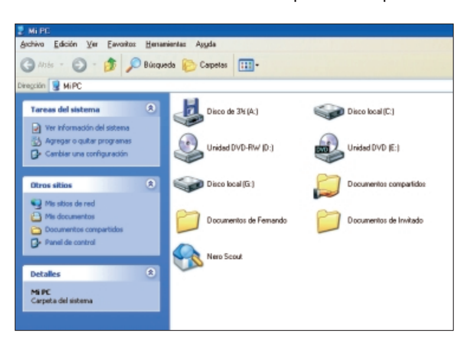
Movimientos más allá de la red local

Algunas veces es posible que quieras compartir información no sólo con los usuarios que están conectados a tu red local sino con los usuarios de Internet. ¿Qué puedes hacer? Lo primero de todo es obviar la el modo estándar de Windows para compartir archivos, ya que no resulta apropiada para las conexiones a Internet. La fórmula indicada para compartir pasa por configurar un servidor FTP. Así, los usuarios pueden conectarse a este servidor utilizando un cliente FTP. Y es que los numerosos servidores FTP, al igual que sus clientes, están disponibles de manera gratuita. De todas maneras, recuerda que la ejecución de un FTP significa que tienes que mantener encendido el ordenador todo el tiempo. Por esta razón, podría ser una buena alternativa alquilar un espacio de archivo en un FTP remoto, aunque también existe la opción gratuita. El servicio Google Mail ofrece una gran cantidad de espacio para esta tarea. Con la herramienta Gmail Drive accedes a éste (**www.viksoe.dk/code/gmail.htm**).

Usando *Documentos compartidos* »

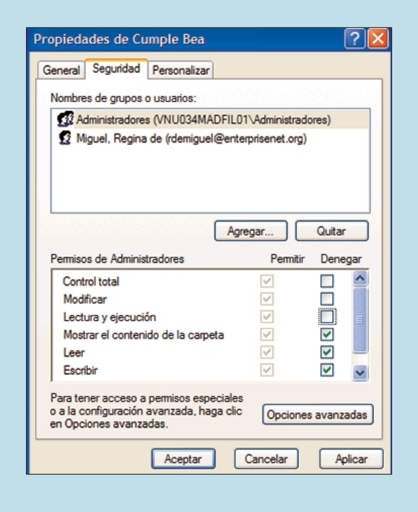
Intercambiar datos

Documentos compartidos es una carpeta especial que pertenece a las distintas personas que utilizan el mismo ordenador, pero que se conectan utilizando diferentes contraseñas. Aunque Microsoft asegura que esta carpeta no se comparte en una red, se trata de una verdad a medias. Si permites compartir archivos y utilizar el Asistente de red, Windows XP automáticamente compartirá *Documentos compartidos* en la carpeta, permitiendo a cada usuario modificar y/o eliminar sus archivos. Si no quieres esto, dirígete a *C:\Documents and Settings\All Users*. Pulsa sobre la carpeta *Documentos compartidos* y escoge, del menú que se despliega, *Compartir y seguridad*. Desactiva la opción *Compartir esta carpeta en la red*. Por otro lado, en un entorno doméstico ¿qué puedes hacer con la carpeta *Documentos compartidos*? Cuando abres *Mi PC*, te encontrarás con un acceso directo a ésta. Por este motivo, resulta conveniente depositar aquí todos tus archivos. Si estás planeando configurar una carpeta para publicar archivos en tu red local, podría ser una buena idea preservar *Documentos ompartidos*.



Entender los NTFS y permisos de red »

Características avanzadas



Estas características únicamente se encuentran disponibles en la versión profesional de XP y sólo cuando la opción del uso compartido simple de archivos está desactivada. De esta manera, la ventana de diálogo de las propiedades de una carpeta tiene dos pestañas separadas: *Compartir* y *Seguridad*. El primero es para configurar los permisos de parte, y la otra para los permisos NTFS. Resulta obvia la idea de que los permisos más restrictivos siempre se aplicarán. Así que si tienes permisos de escritura en una parte, pero únicamente de lectura para los NFTS, no podrás cambiar un archivo. Por defecto, si tú compartes una carpeta, los usuarios solamente tendrán permisos para su lectura. Por esta razón, si alguien quiere crear y guardar archivos en esa carpeta, tendrás que otorgarle los permisos apropiados. Esto puede desalentarte si eres un neófito en temas de redes. Necesitarás conocer a la perfección que significan estos permisos, entendiendo que pueden existir distintos grupos a los que asignar permisos. Para aquellos que no estén muy experimentados, se recomienda el uso compartido simple de archivos.

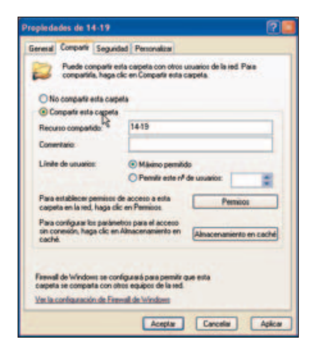


Preguntas y Respuestas

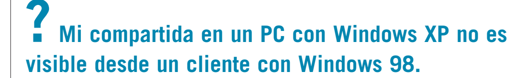
¿Problemas cuando compartes utilizando XP? Nuestros expertos echan un vistazo a algunos de los fallos más molestos e incomprensibles, ofreciendo soluciones rápidas y sencillas.

? Estoy frustrado por las limitadas opciones de Windows XP Home Edition para compartir archivos. Si arrancas tu ordenador en modo seguro o si lanzas el asistente para compartir redes mediante el archivo «shrpubw.exe», consigues el acceso a las opciones estándar para compartir, que te permite configurar los permisos por usuario. Resulta un truco muy útil y me pregunto por qué no se da a conocer mejor.

! Siempre que un usuario remoto tenga acceso a una parte de la versión doméstica de XP a través de la Red, será tratado como un invitado con todos los permisos limitados que esto implica. Ello quiere decir que la citada versión nunca va a distinguir entre usuarios individuales (esto también puede aplicarse incluso su tienes configurado permisos individuales de antemano como nos cuentas). Esto convierte el truco en inútil. Aunque haya dejado constancia de sus permisos, seguramente, nunca se usarán.



Compartir resulta útil. En caso de algún problema, desactiva, reinicia Windows. Haz las comprobaciones necesarias y cambia el nombre. Tus problemas deberían estar resueltos.

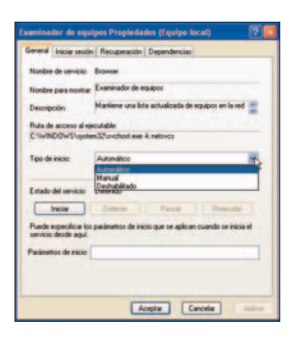


? Mi compartida en un PC con Windows XP no es visible desde un cliente con Windows 98.

! ¿Son visibles para todos clientes XP? Si es así, el nombre que compartes es probable que sea demasiado largo. Windows 2000 y XP pueden manejar nombres de partes extensos, pero las versiones 95, 98 y Me quedan restringidas a un máximo de 12 caracteres. Para una compatibilidad máxima, limita el nombre de la parte a 8 caracteres.

? Me lleva hasta 15 minutos ver las carpetas compartidas de mi red.¿Qué es lo qué está pasando? ¿Existe alguna manera de acelerar esto?

! En un grupo de trabajo dentro de Windows, siempre tienen que haber un equipo como funcione como Maestro, un PC que reconozca las carpetas compartidas y presenta la información a los demás. Cuando varios PCs con Windows están en línea, determinan quien actuará como Maestro. El nuevo Maestro necesita obtener un montón de información que tendrá que pasar al resto de los ordenadores, una tarea que requiere su tiempo. La única manera de acelerar este proceso es excluir equipos individuales de esta elección. Si tienes un PC que siempre está en funcionamiento, éste podría convertirse en un buen Maestro. Ten en cuenta que no serás capaz de acceder a ningún sitio mientras ese equipo no se esté activo. Para descartar un ordenador con XP de esta elección, dirígete a *Inicio*. En *Ejecutar* introduce *services.msc* y pulsa «Intro». Haz doble clic en *Examinador de equipos* y configúralo para que el *Tipo de Inicio* esté *Deshabilitado*. Luego reinicia.

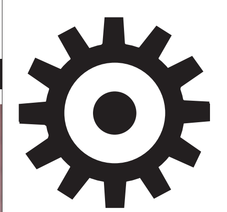


? Cuando mi instalación de red se cayó con Windows 98, tuve que desinstalar y reinstalar TCP/IP. Ahora tengo el mismo problema con Windows XP, pero el botón para desinstalar aparece desactivado. ¿Qué puedo hacer?

! Resetear tu instalación de red TCP/IP es bastante sencillo con XP. Seguimos la ruta *Inicio/Ejecutar* e introducimos *CMD*. Pulsamos «Intro». A continuación, escribimos *netsh int ip reset resetlog.txt* y volvemos a presionar «Intro». En la pantalla verás una línea que hará el mismo trabajo que hiciste cuando desinstalaste y volviste a instalar TCP/IP bajo Windows 98. Si lo deseas, puedes abrir *resetlog.txt* en un editor de textos para controlar el *log* y ver exactamente lo que ha ocurrido. Puedes encontrar información más detallada sobre el proceso en su totalidad en la siguiente dirección: **http://support.microsoft.com/?kbid=299357**.

? Me pregunto cómo de seguros son los archivos que fueron protegidos con permisos NTFS.

! Ante un posible ataque local, prácticamente no hay protección con los permisos NTFS. De hecho, NTFS no es un sistema de archivo que proteja ficheros: son los sistemas operativos los que ofrecen la opción de proteger estos archivos. Si un atacante arranca NTFS Reader (**www.ntfs.com**) o utiliza Linux Live CD, podrán leer y copiar cualquier archivo. La única protección posible en un PC con Windows es EFS, que encripta los archivos y los descifra «al vuelo» cuando un usuario autorizado se conecta.



VOZ SOBRE IP

Nos quedamos asombrados con un ordenador capaz de establecer una conexión de voz con otro... sin pararnos a pensar si ésta era de calidad o no. Hoy en día, la tecnología VoIP se ha convertido en la nueva alternativa de telefonía por Internet. Cuenta con una excelente calidad, buen precio y la posibilidad de utilizar un dispositivo convencional.



La era de la voz sobre Internet ya ha llegado

La telefonía por Internet ha mejorado notablemente desde la aparición de las primeras versiones de las que fuimos testigos en los 90. Hoy en día, la calidad de voz es excelente.

Tras un largo viaje que comenzó en la década de los 90. La tecnología VoIP (*Voice over Internet Protocol*/Voz sobre el Protocolo de Internet) ha alcanzado finalmente el hogar del consumidor. El software dedicado ofrece funcionalidades de telefonía profesionales, DSL nos permite una buena calidad de sonido y requiere un tipo de hardware asequible para aquellos que no puedan estar sin un teléfono convencional. Las redes para VoIP son gratuitas, por lo que son perfectas no sólo para el usuario doméstico sino también para el entorno profesional.

La tecnología VoIP también anuncia un alto potencial económico. Skype prevé unos ingresos de ventas de más de 200 millones de dólares y pronostica un ingreso de ventas de 200 millones de dólares en el 2006. Sin duda alguna la inversión de eBay en Skype de 2,6 billones dará el empujón a al tecnología VoIP.

Skype cuenta con más de 60 millones de usuarios registrados de los que 3 millones utilizan esta tecnología como única forma de conexión. Junto a una de las plataformas de e-commerce más fuertes, Skype se aproxima al estándar abierto SIP del que ofrecen soporte gratuito la mayoría de proveedores de servicios de Internet. Comienza la carrera... en breve sabremos quién será el ganador.

EL LARGO CAMINO HACIA EL ÉXITO A mediados de los 90, la compañía israelí Vocaltec intentó transmitir conversaciones a través de Internet. Debido a las conexiones con poco ancho de banda a través de módem y RDSI, la calidad dejaba bastante que desear. La comunicación se veía fragmentada e incluso era inteligible.

Las redes digitales RDSI, con su capacidad de transmisión de 64 Kbps, eran la mejor alternativa. Los códecs, como PCMA o PCMU, presentan una calidad muy similar a la de RDSI pero requieren un ancho de banda de 80 Kbps en cualquier dirección. Y como el ancho de banda de las conexiones



Cada vez más y más routers cuentan con puertos para teléfonos regulares para poder soportar VoIP.

“La telefonía tradicional tiene los días contados”

RDSI es de tan sólo 64Kbps, la tecnología de VoIP era solamente posible a una calidad de voz reducida. Solamente con la llegada de DSL fue cuando VoIP pudo comenzar a avanzar. Así, lo mejor será invertir nuestro dinero en un paquete que únicamente nos facture por el volumen de datos. Además teniendo en cuenta que un minuto de conversación son 1,2 Mbytes, podremos saber en todo momento a cuánto asciende nuestra factura. Si utilizamos 1 Gbyte de nuestra tasa de volumen de 2 Gbytes, podemos realizar unas 14 horas en llamadas con el Gbyte que queda. Las tasas de tiempo no son la mejor opción, ya que solamente con una conexión on-line permanente un teléfono IP es capaz de reemplazar una línea de tierra, pero si pagamos por tiempo nos supondrá bastante dinero.

LA TECNOLOGÍA VOIP El paquete de transmisión es la base de la telefonía IP. Esta tecnología divide cualquier archivo en pequeños paquetes que se envían al receptor a través de Internet. El software es el encargado de reunir los paquetes en uno solo dependiendo del tipo, de este modo se consigue una capacidad lineal que nos es posible con un circuito de teléfono convencional.

El único problema está en las transmisiones a tiempo real, donde la conexión tiene que ser instantánea. El oyente detectará ciertos retardos de muchas veces 200 milisegundos. Tan pronto como esté disponible el ancho de banda, IP hace frente a estas demoras, que serán tan cortas que casi no podremos apreciarlas. Y lo mejor de todo, IP es económico y en muchas ocasiones gratuito. Una prestación valorada por los usuarios norteamericanos que realizan un 30% de sus llamadas a través de VoIP.

El componente imprescindible es el software capaz de unir los paquetes y formar una llamada de voz legible. Normalmente toma la forma de un teléfono virtual en nuestro ordenador, normalmente un cliente Skype o SIP como X-Lite o SIPPS. Al igual que si de una conexión de Internet se tratara, necesitamos un micrófono y un altavoz que reemplace nuestro receptor de teléfono. Lo mejor va a ser hacer uso de un conjunto de auriculares y micrófono pero es posible también realizarlo utilizando los altavoces del ordenador y una cámara web que incorpore un micrófono.



Los móviles WLAN son la opción más cómoda para telefonía por Internet.

Un conjunto de auriculares y micrófono para VoIP



Nos permite realizar una comunicación en dos sentidos, lo que también se conoce como llamadas *full-duplex*. Este tipo de dispositivo cumple con cada uno de los requerimientos de la telefonía por Internet a través de un software como Skype o SIPPS. Su papel es el mismo que el de un receptor de teléfono.

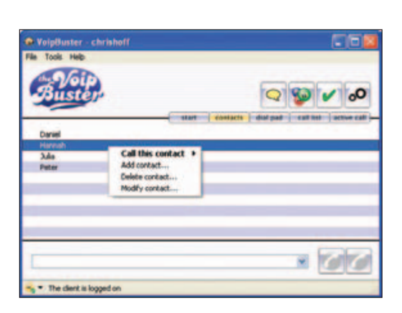
La telefonía en Internet, al alcance de cualquier usuario

Hasta hace poco, las llamadas sobre TCP/IP requerían un proceso complicado. Pero ya no. Skype y otros programas de voz sobre IP son sencillos y baratos.

Llamadas a Europa y Estados Unidos por una suscripción de 10 euros »

VoipBuster

Con el software VoipBuster puedes hacer llamadas sin cargo a teléfonos fijos de doce países europeos y Estados Unidos. Pero las llamadas se cortan tras 60 segundos y tienes que volver a marcar. Este corte se puede evitar con una suscripción de 10 euros. Puedes encontrar las tarifas actuales para llamar a otros países en



www.voipbuster.com/en/rates.html. VoipBuster es más barato que muchos proveedores de telefonía por Internet. El software, parecido a Skype, te permite añadir números de teléfono como contactos e inicia llamadas con un solo clic de ratón. VoipBuster lista todas las llamadas realizadas y se puede actualizar *on-line*. www.voipbuster.com

Una VoIP más conveniente »

Snom 360 Softphone

Si te parece demasiado austero el aspecto general de los clientes VoIP, echa un vistazo a Snom 360 Softphone, un software gratuito para uso privado. Como el hardware original, posee una amplio panel de control con 47 entradas y y una pantalla gráfica. Las doce teclas programables, que se pueden utilizar para personalizar el software, son un punto a su favor. El programa trabaja tras un cortafuegos y soporta *Network Address Translation*. Tras instalarlo, introduce los datos de tu cuenta SIP y ya estará listo para usar. Puedes añadir siete proveedores de VoIP, con cinco mostrados al mismo tiempo. A través de su navegador puedes acceder a los detalles de las llamadas, otras opciones de configuración y funciones de ayuda. incluso puedes usar tonos de llamada diferentes y asignarlos a distintas personas. En conjunto, se trata de un software muy fácil de utilizar. www.snom.com



Teléfono IP con función de vídeo »

Eyebeam

Si quieres llamar por teléfono, chatear y grabar videoconferencias fácilmente, Eyebeam es tu software. Te permite realizar hasta seis llamadas simultáneas o iniciar *conference calls*. Su agenda tiene capacidades como importar y exportar, último número marcado, mostrar todas las llamadas hechas, recibidas y perdidas, así como la grabación de llamadas. Incluso permite dejar llamadas en espera, como una auténtica centralita. Si tienes una webcam conectada, puedes hablar y ver a otros cuatro participantes. Por último, es fácil grabar llamadas y videoconferencias. www.xten.com



Grabar llamadas de Skype »

Hot Recorder

¿Quieres grabar tus llamadas de Skype? Hot Recorder es tu programa. Esta herramienta graba con tres diferentes niveles de calidad. El reproductor integrado reproduce grabaciones o las envía por *e-mail*. El programa incluye un sencillo contestador y 15 muestras de sonido llamadas Emotisounds, que se pueden reproducir mientras se llama. Hot Recorder no sólo trabaja con Skype, sino también con otras herramientas de VoIP. La versión Premium (sin publicidad y con un conversor de audio incluido) cuesta 15 dólares (aprox. 12 euros). www.hotrecorder.com






Softphone para Windows, MacOS X, Linux y Pockect PCs »

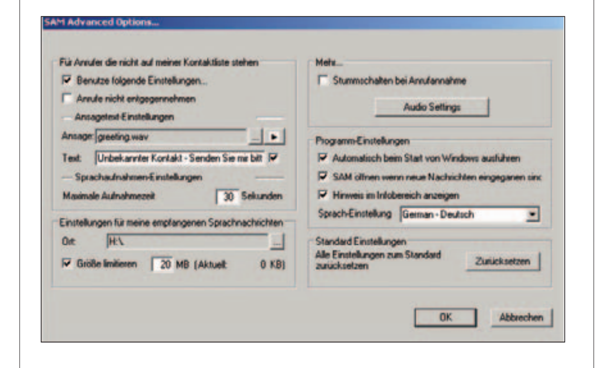
X-Lite

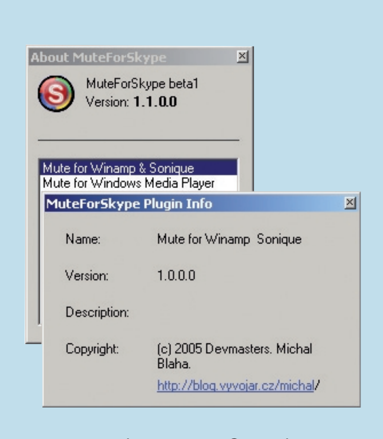
X-Lite ya viene configurado para muchos proveedores de VoIP. Como X-Lite se basa en el estándar abierto SIP, trabajará con cualquier otro proveedor de servicios SIP. Gracias a sus nuevos algoritmos de compresión, proporciona una buena calidad de sonido. La versión X-Pro (20 euros) contiene el códec G.729ª, que proporcina buena calidad en conexiones de banda estrecha, como módems tradicionales. Además, la versión comercial proporciona funciones telefónicas extendidas, incluso para Pocket PCs. Junto a una red inalámbrica, el Pocket PC se convioerte en un teléfono inalámbrico. Para X-Lite funcione bien, debes abrir los puertos 5061 y de 8000 a 8005 en tu cortafuegos. La primera vez que lo utilices, un asistente te guiará a través de la configuración del audio y lo calibrará para evitar ecos y otras distorsiones durante la reproducción. **www.xten.com**

Contestador telefónico gratuito »

SAM

Skype proporciona un contestador llamado Voicemail por un precio de 15 euros al año (o 5 por tres meses). los usuarios de VoIP que necesiten un servicio contestador deberían probar el contestador gratuito de Skype, SAM. Éste tiene todas las funciones básicas de un contestador, como mensaje de bienvenida o ajuste de los tiempos de grabación. El programa puede diferenciar entre las llamadas entrantes (las que están en tu lista de contactos y las que no) y reproducir diferentes mensajes para cada grupo. **www.doubleglick.com**





Silencia el audio con llamadas entrantes »

Mute for Skype

Si te gusta escuchar música mientras trabajas, necesitas Mute for Skype. Este software gratuito corre de fondo y monitoriza el software VoIP, incluyendo Skype y muchos otros. Cuando entra una llamada y es respondida, esta pequeña utildad entra en acción. Pausa automáticamente la cualquier reproductor, desde Windows Media Player a Winamp, de modo que la llamada no se vea interrumpida. Después de cerrar la conexión de VoIP, la herramienta vuelve a activar la reproducción de música. Para poder utilizar Mute for Skype, debes instalar Microsoft .NET Framework 1.1 en tu PC. Se puede cargar mediante las actualizaciones de Windows.
blog.vyvojar.cz/michal/articles/3494.aspx



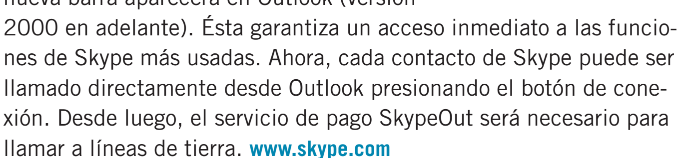
Cuidado con la compatibilidad »

Teléfonos IP

No todos los teléfonos IP se ajustan a los estándares reconocidos. Así, antes de comprar uno, asegúrate de que podrá trabajar con tu proveedor SIP. Las marcas más conocidas son compatibles con SIP. utilizan perfiles reconocidos y son capaces de trabajar con la mayor parte de los proveedores de estos servicios. Los proveedores normalmente ofrecen extensas instrucciones y trucos de istalación para los dispositivos más comunes en sus páginas web. Ten cuidado con las compras que haces en páginas como eBay!, pues muchas veces ofrecen teléfonos IP Cisco, cuando no son compatibles con SIP.

La mejor conectividad »

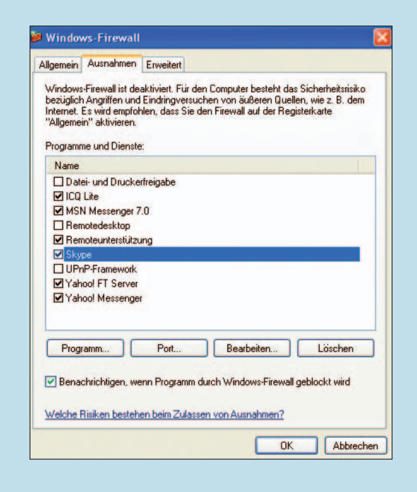
Skype for Outlook



Microsoft Outlook es casi un estándar para la gestión de contactos, mientras Skype es la más mpopular herramienta de VoIP. Skype for Outlook es un *add on* gratuito que une ambas aplicaciones, proporcionando características telefónicas. Tras la instalación, una nueva barra aparecerá en Outlook (versión 2000 en adelante). Ésta garantiza un acceso inmediato a las funciones de Skype más usadas. Ahora, cada contacto de Skype puede ser llamado directamente desde Outlook presionando el botón de conexión. Desde luego, el servicio de pago SkypeOut será necesario para llamar a líneas de tierra. **www.skype.com**

Una correcta configuración mejora la VoIP

Firewall software



Los usuarios de Skype con el Firewall de Windows XP SP2 deberían hacer algunas comprobaciones básicas. En la pestaña *General*, asegúrate de que la opción *No permitir excepciones* está desactivada. Es muy importante permitir excepciones, pues el cortafuegos de Windows bloqueará si no todos los intentos de acceso sin preguntártelo. Skype ya debería estar listado en *programas y servicois* de la pestaña *Excepciones*. Si no, tienes que añadir manualmente el programa de VoIP. Presiona el botón *Agregar programa* y selecciona Skype en la lista *Programas*. Ahora presiona *Modificar* y *Cambiar ámbito* en la siguiente ventana. La opción más indicada en este caso es *Cualquier equipo (incluyendo los que están en Internet)*. Cierra todas las ventanas de diálogo presionando *Aceptar*. De esta maner, el Firewalll de Windows se puede configurar para trabajar con distintos software de VoIP, como ACQ, AOL Instant Messenger, Yahoo Messenger y Windows Messenger. Muchos usuarios no utilizan el Firewall de Windows y confían su seguridad a aplicaciones externas como Zone Alarm, Norton Personal Firewall o McAfee Firewall. La configuración para cada uno de ellos sólo es ligeramente diferente, de modo que la configuración de Zone Alarm (**www.xonelabs.com**) puede servirnos como referencia para los demás. Normalmente, sólo es necesario hacer dos clics de ratón decirle al firewall que cierto software debería tener siempre acceso a Internet. Cuando arranques Skype, por ejemplo, Zone Alarm muestra un mensaje de advertencia de seguridad. Esta ventana te comunica que el archivo «skype.exe» quiere acceder a Internet. Selecciona la opción *Remember this setting* y confirma presionando *Allow*.



Videoconferencias con Skype »

vSkype

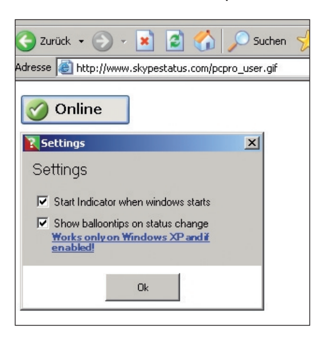
Sorprendentemente, Skype es de los pocos que carece de características de transmisión de vídeo. Para poder disfrutar de videoconferencias (con hasta 200 participantes) con esta aplicación, necesitaremos un programa como vSkype. Su manejo es muy sencillo. Selecciona todos los contactos que vayan a participar en la videoconferencia y haz clic en *Start* para enviar una invitación a todos los participantes. Si es necesario, la aplicación muestra ventanas individuales o todo el escritorio de otros usuarios. De este modo, todos los usuarios conectados podrían, por ejemplo, ver un documento. **www.vskype.com**



Muestra el estado de Skype en la Web

Indicador de estado on-line

La herramienta Skype muestra tu estado en línea (por ejemplo, «fuera», «no molestar» o «no disponible») sólo a otros usuarios que te tengan en su listado de contactos. Si quieres mostrar tu estado de forma independiente de la lista de contactos, necesitas la herramienta gratuita Skype Online Indicator. Esta aplicación determina tu estado on-line y lo muestra gráficamente en **www.skypestatus.com**. Así, podrás publicarlo en páginas web o en foros de discusión. La aplicación requiere que tengas instalado en tu ordenador la versión 1.1 o superior del software de Microsoft .NET Framework. **www.skyperunners.com**



Preguntas y Respuestas

VoIP y Skype no son lo mismo. Ambos ofrecen llamadas de teléfono a través de Internet a bajo precio, con distintos niveles de usabilidad y seguridad. Te ayudamos a elegir la que más se adecua a tus necesidades.



Los usuarios de Skype que utilizan algún tipo de software para hablar por chat a través del teclado pueden conseguir divertidos efectos visuales con Skype 3D Avatar en www.vaka.com.

Códigos de error VoIP

Código	Descripción
200	OK
301	Trasladado permanentemente
302	Trasladado temporalmente
400	Petición fallida
402	Se requiere pago
403	No permitido
404	No encontrado
405	Método no permitido
406	No aceptable
407	Se requiere autentificación del proxy
408	Petición de espera
410	No se encuentra
413	Petición de entidad demasiada larga
480	No disponible temporalmente
484	Dirección incompleta
487	Petición finalizada
500	Error del servidor interno
502	Salida fallida
503	Servicio no disponible
504	Servidor en espera
505	Versión no soportada
600	Ocupado
604	No existe

? ¿Cómo puedo enviar mensajes automáticos con Skype?

! El programa freeware Jyve amplía las características de Skype con una serie de prácticas funciones. La función *Auto Responder* es muy útil para usuarios habituales. Con ella es posible enviar respuestas automáticas a nuestros contactos. El programa detecta automáticamente si el usuario no se encuentra disponible, bien para realizar una llamada, bien para recibirla de un usuario que no está en nuestra lista. De este modo envía el correspondiente mensaje de texto. **www.jyve.com**

? ¿Puedo realizar una llamada a través de Skype desde cualquier explorador?

! La barra de herramientas de Skype es extensible a las funciones de Windows Internet Explorer 5.0 ó superior bajo Windows XP. Esta barra proporciona acceso rápido a las funciones más importantes de Skype. Así por ejemplo podemos cambiar nuestro estatus *on-line*, visualizar la lista de contactos e iniciar llamadas a través de Internet con tan sólo un clic de ratón. Además, reconoce números de teléfono así como nombres de usuarios de Skype. **www.skype.com**.

? ¿Cómo configurar mi router para VoIP?

! Como el router diferencia entre una red local e Internet, tiene que ser informado sobre dónde han de enviarse los paquetes de datos entrantes. La solución está en redirigir los datos entrantes en un puerto específico, normalmente UDP 5060, a otro ordenador de la red local. Debido a que las características e interfaces de configuración difieren de un router a otro, y a que todas las herramientas de VoIP utilizan distintos puertos, no será demasiado difícil este procedimiento. El router debería trabajar con la mayoría del firmware, pero siempre tenemos la posibilidad de actualizarlo.

? Utilizo varios dispositivos SIP junto con un router, ¿debo tomar alguna precaución?

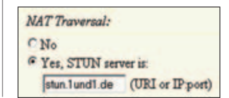
! Cuando hacemos uso de varios dispositivos SIP al mismo tiempo, cada teléfono VoIP deberá disponer de una dirección IP estática. Si por ejemplo utilizamos un nuevo hardware Grandstream BT-101, podemos realizar un cambio en la configuración de la dirección IP o bien utilizar la interfaz de configuración; tendremos que ajustar los puertos utilizados al router. El hardware Sipgate se configura por defecto en los puertos 5004 (RTP) y 5060 (SIP). Si los dos dispositivos se encuentran en uso, el segundo pasará al puerto 5005 RTP; el nuevo puerto SIP es 5061. Para cada componente adicional de hardware VoIP, ambos números de puerto se incrementarán en uno. Por último, el router tendrá que reconfigurarse: los puertos 5005 y 5061 tendrán que redirigirse a la dirección IP del correspondiente dispositivo SIP. Repetimos este procedimiento para cada dispositivo VoIP.

? ¿Es segura la Telefonía IP?

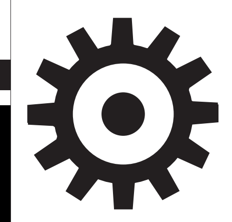
! Las conexiones de voz a través del protocolo SIP no son encriptadas, por lo que debemos ser cuidadosos a la hora de introducir nuestro número PIN en el teclado del teléfono. Cuando recibimos llamadas a través de una estación remota fija (como pueda ser a través de nuestro banco), podemos cambiar a una conexión VPN. Esta conexión encripta el tráfico completo de datos en ambas direcciones, incluyendo los paquetes VoIP. Otra opción va a ser utilizar Skype (**www.skype.com**). Este software trabaja con un protocolo propietario encriptado.

? ¿Qué significa un código de error?

! Si no se oye ningún tipo de tono de marcación o tono de ocupado, los teléfonos VoIP a menudo visualizan un código de error. Estos mensajes están normalizados para el protocolo SIP. Podemos encontrar una lista con todos los códigos de error en **www.voipinfo.org/tiki-index.php**. También aquí incluimos una pequeña relación de los códigos más importantes.



Con Stun evitamos cualquier mensaje de error durante la conexión a un servidor SIP.



STREAMING

Finalmente todo nos llega junto. Las ultrarrápidas conexiones de banda ancha, TV, radio, películas y música a través de la red, software de reproducción cada vez más rápido y más manejable, y un hardware cada vez más integrado en nuestro hogar por su atractivo diseño son las claves de lo que se denomina *streaming*.





Disfruta de la música y las películas a través de la red

Las conexiones DSL acercan la emisión de vídeo en tiempo real a nuestra casa y dan acceso a las estaciones de radio web. *Streaming* es la respuesta para el ocio del siglo XXI.

El *streaming* nos proporciona contenidos multimedia en la pantalla de nuestro ordenador, en nuestro sistema de alta fidelidad, aparato de TV y ahora en algunas consolas de videojuegos. Pero, ¿cómo trabaja?

Para simplificar, un servidor conectado a una red de área local o a Internet, enviando de forma constante archivos de audio o vídeo. El cliente de *streaming* -nosotros- accede al caudal de datos, decodifica el contenido en el medio que se haya enviado y lo reproduce. Esta actividad no saturará nuestra red ya que los datos están comprimidos, generalmente por un algoritmo relativo al MPEG, en especial si se trata de archivos de vídeo. En lugar de grabar cada *frame* o fotograma recibido, lo que consumiría nuestro disco duro en poco tiempo, se almacenan los cambios entre un *frame* y el siguiente. En muchas escenas, el fondo se mantiene fijo mientras la acción se desarrolla en primer plano. En este caso, grabar todos los fotogramas sería un desperdicio de espacio en disco duro y de recursos.

CONECTA LA TV A UNA SINTONIZADORA de televisión vía satélite y podrás observar las excelencias de esta nueva forma de emisión televisiva. En los paisajes y en aquellas escenas tranquilas, la calidad de la imagen es realmente brillante. Si embargo, en las escenas de acción con rápidos cambios de plano, si observamos la imagen de cerca encontraremos pixelación y pequeños artefactos. Este efecto es más evidente en las transmisiones a través de Internet. Esto es debido a que las estaciones de transmiten los datos con un alto índice de compresión. En cualquier caso, las emisiones a través de la Red tienen una calidad similar a la de las emisiones de TV. Si el servidor de *streaming* está conectado directamente a nuestra red de área local, la calidad de las emisiones tiene como único límite las características técnicas del propio cliente.

Las emisiones de radio generalmente tienen buena calidad de sonido, dado que los archivos de audio son más pequeños que los de vídeo. Si embargo, este tipo de archivos también se les aplica un algoritmo de compresión para reducir su tamaño, eliminando aquellos elementos que no detecta el oído humano. A este tipo de compresión se la denomina compresión con pérdida.

El teclado de Microsoft está especialmente diseñado para los PCs con Media Center, lo que nos permite controlar los distintos accesorios adicionales, no sólo los que trabajan con este módulo del sistema operativo.





“Escucha el suave sonido del *streaming*”

Desde el punto de vista técnico, vídeo bajo demanda difiere radicalmente de la emisión en *streaming*. Los proveedores de vídeo bajo demanda utilizan un pequeño truco para proporcionarnos una retransmisión más regular. La primera parte de la película se transfiere sin que haya empezado a reproducirse y no comenzará a hacerlo hasta que se haya almacenado en el *buffer* la cantidad de película suficiente. Suficiente significa que debe dar tiempo a que se descargue la segunda parte mientras estamos visionando la siguiente, y así sucesivamente.

EL HARDWARE NECESARIO depende del medio elegido. Un adaptador RDSI nos valdría para las emisiones *on-line* de la radio, pero con algunas limitaciones. Sólo un ratio de descarga sostenido de 128 Kbps, nos ofrecería una calidad aceptable. Para poder acceder a archivos de vídeo o de audio de alta calidad, debemos contar con una conexión ADSL.

En todas estas actividades es necesario contar con una tarjeta de sonido de medianas características, todos los PCs cuentan con una, y con una tarjeta gráfica que sea capaz de trabajar con gráficos 3D, es decir, cualquier PC que tenga cuatro años o menos. Para tener una buena recepción de imágenes estáticas necesitaremos unos 150 Kbps, y para *streaming* de vídeo es recomendable contar al menos con unos 300 Kbps.

También es necesario software de reproducción. Windows Media Player recibe a la perfección emisiones de radio y televisión en Internet, aunque si los datos son enviados en los formatos RealAudio o RealVideo, la aplicación necesaria será RealPlayer.

CREAR NUESTRA PROPIA ESTACIÓN de emisión en una red, transmitiendo contenidos a los ordenadores conectados a ella es relativamente sencillo. Esto significa que puedes ver el último éxito en tu portátil en el jardín o mostrar una película en varias habitaciones a la vez. Pero no contamos con un PC instalado en cada habitación, afortunadamente existen soluciones más elegantes para acceder al lugar dónde tengamos almacenados los cientos de temas en MP3 y las distintas secuencias de TV que hayamos grabado.

El software apropiado permite a los clientes acceder a los archivos almacenados y activar funciones de búsqueda. Las comunicaciones se pueden realizar a través de una red convencional o wireless. El sistema de distribución es muyescalable. A través de este sistema, cada miembro de la familia puede acceder a distintos contenidos desde su habitación con su cliente personal, por ejemplo una XBox.

Las redes convencionales, por cable, cuentan con una pequeña ventaja respecto a las redes wireless. Estas ofrecen un ancho de banda de 54 Mbps, lo que no es suficiente para el *streaming* de películas en formato DVD o MPEG-2, especialmente si más clientes están generando tráfico adicional. Las líneas PLC son una solución parcial ya que nos ofrecen un ancho de banda de 85 Mbps a través de la red que nos proporcionan los enchufes de nuestra casa.

XBox no sólo es una consola para juegos. Si reconoce un Media Center ejecutándose en la red en la que está conectada, le proporciona las fotos, vídeos y archivos de audio vía streaming, además de funcionar como grabador de vídeo.







Los fabricantes como Dell están evolucionando con el tiempo. Los diseños cada vez se adaptan más a la integración de los PCs en el salón. Productos como el Dell 5150C o la XBox son un buen ejemplo de ello.

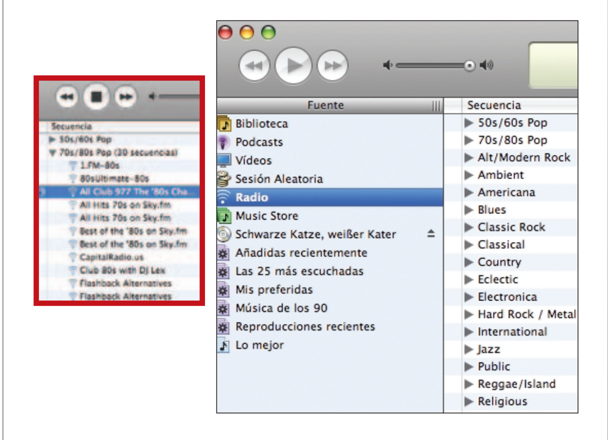
Cuando quieras, donde quieras... pincha audio y vídeo

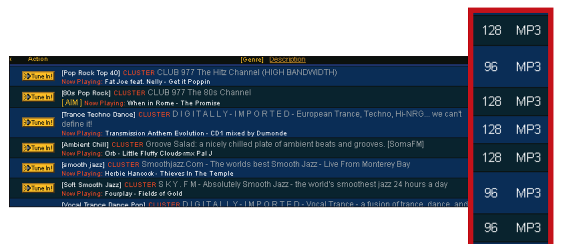
No sólo debes limitarte a almacenar música en MP3 y vídeos en DivX en tu disco duro. UPnP a través de una red permite la transferencia de TV,

Grabando radio de la web »

iTunes

Tanto para los usuarios de Mac o PC, iTunes es una aplicación muy útil para la reproducción y gestión de archivos. Simplemente hacemos clic en el icono Radio en la barra de navegación de la izquierda y se desplegará una lista de las estaciones de radio disponibles con diferentes calidades. Como iTunes no cuenta con la función de grabación, necesitamos la instalación de un software adicional como Tunebite.





No menos de 128 Kbps »

Grabando radio de la Web

Cuando grabamos las emisiones de radio de Internet debemos prestar atención al régimen de transferencia. Muchas estaciones emiten a una calidad insuficiente, sólo una calidad de sonido de 128 Kbps o superior es suficiente para disfrutar de la música de un reproductor de audio o en un equipo de alta fidelidad.



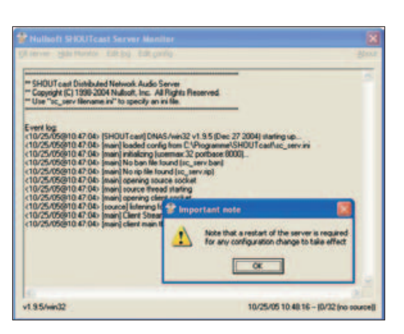
Conectarse a un grabador con disco duro »

Servidor de *streaming*

Los usuarios del grabador de vídeo Kiss DP-558 pueden acceder al interior del disco duro que integra a través de un cliente FTP y también acceder a todos los programas almacenados en formato MPEG-2. Si la cuenta FTP la tenemos mapeada en memoria como una unidad de red con Windows XP, un servidor de streaming está disponible para ofrecer sus archivos a todos los dispositivos conectados a la red. Para ello debemos iniciar el asistente para añadir sitios de red. Esta operación la podemos realizar desde el explorador de Windows a través de la opción de menú *Herramientas/Conectar unidad de red* y marcamos la casilla *Conectar de nuevo al iniciar sesión* y hacemos clic en la opción *Subscribirse a almacenamiento remoto o conectarse a un servidor de red*. Como la mayoría de las aplicaciones que trabajan como servidor de *streaming* sólo reconocen las unidades de red con una letra. Para ello necesitamos un cliente FTP como Webdrive.

Nuestra propia estación de radio »

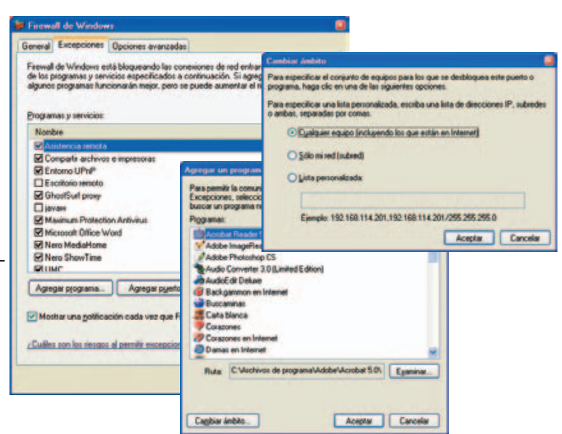
Casi todos los clientes de streaming reproducen la radio vía web. Muchas estaciones de radio emiten en los formatos WMA o Real. Pero sólo algunos dispositivos los soportan a los dos. Pero Shoutcast (**www.shoutcast.com**) nos proporciona el acceso a muchas emisiones de radio en Internet. Trabaja en las tres plataformas y para su uso doméstico basta con que tengamos un PC y una sintonizadora de radio. Este software apenas consume recursos y la programación de radio se emite en MP3.



Abrir los puertos del firewall »

Clientes de *streaming*

Si el cliente de *streaming* se empeña en no detectar al servidor, el problema en la comunicación suele estar en el cortafuegos. Con el Firewall de Windows XP, los canales de datos UPnP se pueden abrir de la siguiente manera. Selecciona *Firewall de Windows* en el *Panel de Control*. La elección que debemos realizar está en la pestaña de *Excepciones*. Pulsamos en el botón *Añadir programas* y abrimos la ventana de *Agregar programas*. En ella, las opciones de búsqueda nos permiten localizar y desbloquear el servidor UPnP. Con otro cortafuegos que nos permita excepciones sólo a nivel de puertos, la aplicación de seguridad tiene que permitir la transferencia de datos por el puerto 1900 así como los que van desde el 49152 al 49154.





Búsqueda por artista »

Shoutcast radio web

Es posible que estés desesperado buscando un artista o grupo concreto, puedes servirte de esta aplicación, más concretamente puedes utilizar el motor de búsqueda que encontramos en su web, **www.shoutcast.com**. Simplemente basta con que escribamos el nombre del grupo en el campo de búsqueda amarillo situado en el margen derecho. En la mayoría de los casos la búsqueda nos da como resultado alguna estación de radio que la esté reproduciendo en ese momento.



Reinicio de la función UPnP »

Windows Media Player

Aunque Microsoft cuenta con un servidor UPnP gratuito para los clientes de *streaming*, Windows Media Player todavía no es capaz de trabajar con él. El *plug-in* gratuito On2Share elimina este problema. Después de la descarga desde la web **www.on2share.com**, la función la podemos activar desde Herramientas/Complementos en el menú de Media Player. Entonces On2Share automáticamente realizará una búsqueda de los servidores disponibles. Si lo deseamos, podemos añadir estos archivos a la librería de Windows Media Player.

Reducir el consumo de energía »

Servidores de *streaming*

El funcionamiento de un ordenador permanentemente encendido proporcionando archivos para uno o más clientes de *streaming* provoca un ruido que puede acabar con la paciencia de más de uno. Los dispositivos NAS pueden ser la solución al problema. Este tipo de dispositivos cuentan con un disco duro o cuenta con puertos USB para conectar discos externos. Pero para cada cliente es necesario el software adecuado. Si el reproductor se sirve del protocolo UPnP, Twonkyvision Mediaserver es el software ideal. Este software nos permite la posibilidad de trabajar con nuestro PC y con una larga lista de dispositivos NAS. Además de una versión de pago de vídeo, fotografías y audio, el servidor está también disponible en su versión gratuita. Mac mini es otra alternativa a los PCs más ruidosos, ya que su ventilador sólo entra en funcionamiento en determinadas ocasiones.



Si instalas un cliente VNC en tu Mac mini, no necesitas ni el ratón ni el teclado, puedes servirte del mando a distancia cómodamente desde el sofá. Si el espacio en el disco duro se reduce rápidamente, puedes conectar rápidamente un disco duro externo adicional a través de los distintos puertos USB o Firewire.

Clientes de *streaming* de audio: Philips WACS700



Este producto de Philips fue una de las grandes estrellas de la pasada feria IFA de dispositivos digitales.

Una de las novedades que se han presentado en el IFA celebrado en Berlín este año con más fuerza ha sido el modelo WACS700 de Philips. Funcionalmente se trata de un dispositivo comparable al Yamaha Musiccast System con la ventaja de ser bastante más barato. Su aspecto es similar a cualquier sistema de alta fidelidad convencional, cuenta con sintonizadora de radio y reproductor de CDs y dos altavoces. Pero además cuenta con un disco duro de 40 Gbytes, conexiones Ethernet y Wireless LAN. Una de las operaciones más interesantes es la posibilidad de introducir un CD con archivos MP3 en el reproductor y transferir todo su contenido al disco duro. Si los archivos de este CD estuviesen en CD Audio, WACS700 convertiría en tiempo real los archivos en formato MP3 para ahorrar espacio en el disco de destino. Simultáneamente, este sistema otorga nombre al álbum y a las canciones gracias a las etiquetas ID3 y a la base de datos que integra el dispositivo.

A la hora de grabar música desde un CD, tenemos dos posibilidades: la primera de ellas es realizarlo mientras escuchamos el CD, velocidad de 1x y la segunda sería hacer una copia de seguridad en nuestro disco duro, que se realiza a una velocidad de 4x. De hecho, en el momento que leamos HD en la pantalla del dispositivo, significa que podemos acceder a los temas almacenados en el disco y crear listas de reproducción en base a los artistas o el nombre de las canciones. El control remoto en este sentido es muy completo, ya que nos permite realizar casi cualquier operación de todas las posibles que ofrece el sistema.

El acceso a los diferentes modos de trabajo se realiza pulsando varias veces, en función del modo al que queramos acceder, sobre el botón de encendido. A través de él llegamos al sintonizador de radio *on-line* con el accederemos a las 40 estaciones de radio almacenadas. Pulsándolo una vez más, se activará el modo auxiliar. Si tenemos conectado un reproductor MP3 al conector RCA, este dispositivo es capaz de reproducir los archivos almacenados en él.

Cualquier fuente de audio, CDs, radios *on-line*, etc, es susceptible de ser grabada en el disco duro. Una vez allí podemos renombrarlas, cambiar atributos como el nombre o el artista y borrarlas si así lo creemos oportuno. Otra de las posibilidades es conectar nuestro PC al WACS700 vía Ethernet.

La grabación la podemos realizar desde cualquier modo, menos en el modo HD como es lógico. El producto cuenta con un gestor denominado Digital Media Center, al que podemos acceder desde el PC, ya sea vía Ethernet o Wireless. Gracias a este gestor, podemos añadir otras cinco estaciones.

Los usuarios del protocolo UPnP están de enhorabuena, ya que el dispositivo de Philips es capaz de trabajar con él, lo que nos posibilita el intercambio de información con otros productos que lo soporten, como el dispositivo de Netgear, también analizado en estas páginas.

Respecto a la calidad del sonido de los altavoces integrados, es realmente sombrosa, más si le añadimos un amplificador auxiliar. ■

CARACTERÍSTICAS

FABRICANTE: PHILIPS
PRODUCTO: WACS700

- » Formatos de audio: MP3 y WMA
- » Régimen de transferencia: 16-320 Kbps +VBR
- » Radio *on line* y sintonizador
- » Amplificador: 2 x 20/ 2 x 80 watios
- » Entradas y salidas analógicas
- » Dimensiones: 360 x 128 x 283 mm (cliente)
- » 608 x 175 x 303 (servidor)

PRECIO Y CONTACTO:

- » Precio: 882,81 euros
- » Web: www.audiotronics.es

VALORACIÓN

Diseño atractivo, funcionalidad y gran calidad de sonido hacen de este producto uno de los más recomendables.

★★★★★



Yamaha MCX-A10/MCX-1000





El producto que nos ocupa de Yamaha se puede decir que integra dos dispositivos en uno. Por un lado contamos con el dispositivo central, MCX-1000, que posee un disco duro de 80 Gbytes y una unidad de regrabación CD-RW. Con estos dos dispositivos podemos almacenar una colección de audio de 1.000 CDs en el disco en formato MP3 con una calidad de 160 Kbps. A través de ellos también podemos extraer o «ripear» la música de un CD y guardarla en el disco duro a una velocidad de 8x. Los datos de los archivos de audio grabados en el disco los podemos clasificar atendiendo a los artistas o al nombre de álbum gracias a la base de datos que almacena. Otra de las ventajas es la posibilidad de obtener música de fuentes externas gracias a sus entradas de audio. También cuenta con una entrada para teclado lo que nos facilita renombrar los archivos que vayamos introduciendo en el disco. También cuenta con conexiones VGA y S-Vídeo, lo que nos facilita conectar un monitor de ordenador o un aparato de televisión.

Respecto al cliente, MCX-A10, tiene un aspecto similar al de cualquier cadena de música estéreo. La comunicación con el servidor, MCX-1000, se puede realizar por Ethernet o WLAN. Por medio de su pantalla LCD y el panel de control podemos realizar multitud de operaciones, entre ellas borrar canciones. Del mismo modo, el mando a distancia nos ofrece una gran variedad de posibilidades.

Una de las características que nos ha parecido más interesante es el modo *Party*. Permite limitar, siempre desde el servidor, algunas funciones como la escritura en disco. Este modo también nos posibilita colocar en las salidas del servidor los archivos que queramos compartir con el resto de clientes que estén conectados en ese momento.

El servidor tiene una capacidad para comunicarse con tres clientes vía *wireless* y otros dos por cable de forma simultánea.

El receptor de Yamaha se conecta con el servidor a través de una conexión RS232, por lo que el cliente puede transmitir lo que capte desde una estación de radio *on-line*. Otra opción interesante es la de colocar marcadores en la reproducción, lo que nos permite recuperarla en el mismo punto.

En líneas generales, podemos decir que se trata de un buen equipo para trabajar juntos. ■

CARACTERÍSTICAS

FABRICANTE: YAMAHA

PRODUCTO: MCX-A10/MCX-1000

» Formatos de audio: MP3
» Radio web: No
» Amplificar: 2 canales x 12 watios
» Pantalla LCD: Sí
» Ethernet/Wireless: Sí/Sí (11 Mbps)
» UPnP: Sí
» Entrada/Salida analógica: Sí/Sí
» Entrada/Salida digital: Servidor/Sí
» Dimensiones: 210 x 246 x 130 mm (cliente). 435 x 136 x 435 mm (servidor)

PRECIO Y CONTACTO:

» Precio: 699/2419 euros
» Web: www.yamaha.es

VALORACIÓN

Fácil de usar, aunque sólo trabaja con el servidor adecuado.

★★★★



Los productos informáticos y de electrónica de consumo van de la mano. Este sistema de *streaming* de audio cuenta con disco duro de 80 Gbytes y regrabadora de CDs.

Roku SoundBridge M-2000



El dispositivo de Rokulabs que analizamos en estas líneas lo podemos definir como un puente entre nuestro PC y nuestra cadena de música. Su funcionamiento es muy sencillo. Por medio de la tecnología inalámbrica se conecta con nuestro PC y a nuestro aparato de música.

Su aspecto es realmente atractivo, aunque sin renunciar a su funcionalidad, ya que en su *display* o pantalla podemos observar claramente la información relativa a la música que se está reproduciendo en ese momento, desde el artista o el título de la canción hasta el tiempo de reproducción. Su diseño en forma de tubo nos permite alojarlo cómodamente junto al aparato de música, como si se tratase de un módulo más de la propia cadena de música.

M-2000 establece comunicación con nuestro ordenador por medio del correspondiente servidor software que se comunica a través del adaptador Ethernet o por medio de la tecnología inalámbrica 802.11b, es decir, a un régimen de transmisión de 11 Mbps. Gracias a la herramienta denominada Slimserver, integrada en el dispositivo, cualquier aplicación UPnP es capaz de comunicarse con él y aprovechar todas sus posibilidades, incluidos aquellos que se sirvan de iTunes. La forma de mostrarnos la información puede variar en función del servidor que se esté utilizando en ese momento.

Este dispositivo de Rokulabs cuenta con un gran número de estaciones de radio *on-line*. En combinación con un *router* y un acceso a Internet, la reproducción de cualquier estación de radio web es sencilla. Utilizando como servidor iTunes, podemos reproducir un gran número de emisiones.

La conectividad es otro de los puntos más destacados de este dispositivo. Los diseñadores le han dotado de salidas de audio analógicas y digitales, lo que nos permite conectarlo a un amplificador que las integre. Si quieres utilizar este dispositivo sin conectarlo al aparato de música, podemos conectarle unos altavoces.

El modelo más pequeño, el M-1000, ofrece prácticamente las mismas funciones que las de su hermano mayor, aunque su pantalla es de dimensiones más pequeñas. En esta misma familia encontramos el modelo M-500, más asequible,cuya diferencia principal con los otros dos es que su pantalla tan sólo tiene dos líneas de texto, de 40 caracteres cada una.

El diseño de estos dispositivos nos permite apilarlos gracias al soporte que nos proporciona el fabricante.

El cliente integrado en ellos es capaz de trabajar con archivos con derechos de autor de Microsoft, DRM. Se trata de unos de los clientes que se han actualizado en lo que se refiere a los archivos de música protegidos.

Por medio del servidor SlimServer podemos sincronizar varios clientes simultáneamente, lo que nos permite reproducir varios temas al mismo tiempo. Otros fabricantes denominan a esta función modo *Party*. ■

CARACTERÍSTICAS

FABRICANTE: ROKULABS

PRODUCTO: SOUNDBRIDGE M2000

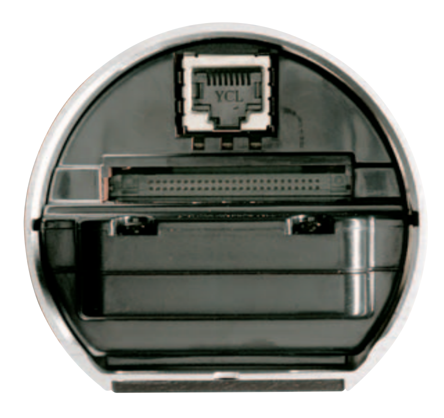
Audio: MP3, MP3pro, WAV, AAC y Ogg
Régimen de transferencia: 16-320 Kbpsw +VBR
Radio web: Sí
Amplificador: No
Ethernet: Sí
Wireless: Sí (11 Mbps)
Salidas analógicas: Sí
Entradas analógicas: No
Salidas analógicas: Sí
Dimensiones: 425 x 75 x 68 mm

PRECIO Y CONTACTO

Precio: 399,99 dólares (vía web)
Web: www.rokulabs.com

VALORACIÓN

Diseño atractivo, sencillo de utilizar e instalar y soporte para un gran número de formatos.
★★★★★





¿Te suenan estas interfaces? La integración entre LAN y el disco duro significa un verdadero encuentro de conexiones de audio y vídeo.



Philips MCW770

La funcionalidad de *streaming* es sólo una de las tres opciones que nos ofrece este modelo de Philips. Cuenta con un cargador de cinco CDs, algo poco recomendable ya que ofrece muchas más posibilidades de error o de que se estropee. El sonido que podemos oír por los altavoces se reproduce en cuatro tonos diferentes gracias al ecualizador digital integrado. Además también integra un amplificador de doble canal con 75 watios por cada canal. Esto nos proporciona una calidad de sonido y una potencia que no se ve disminuida aunque subamos el volumen al máximo.

Su conexión a una red de área local es por medio de tecnología inalámbrica, aunque si nuestra red doméstica no coincide con el estándar de este producto, 802.11b, el fabricante nos proporciona un adaptador USB-WLAN. Los ingenieros de Philips utilizan el software propietario Media Manager como servidor. Esta aplicación nos permite, no sólo enviar archivos de audio a los distintos clientes de *streaming* conectados, sino que nos facilita la organización de nuestros archivos.

Cuando accedemos a una estación de radio *on line*, MCW770 nos la puede agregar a nuestros favoritos pero vía web, es decir, en un área de la web de Philips.

El control remoto de este dispositivo de *streaming* es capaz de realizar todas las funciones integradas. Este detalle es de especial importancia ya que cada vez es una opción más demandada por los usuarios. ■

CARACTERÍSTICAS

FABRICANTE: PHILIPS

» Formatos de audio: MP3, WAV
» Régimen de transferencia: 16-320 Kbps +VBR
» Radio web: Sí
» Sintonizador de radio: Sí
» WLAN: 11 Mbps
» UPnP: Sí
» Entradas analógicas: Sí
» Dimensiones: 175 x 286 x 340 mm (Sistema), 175 x 275 x 242 mm (Altavoces)

PRECIO Y CONTACTO

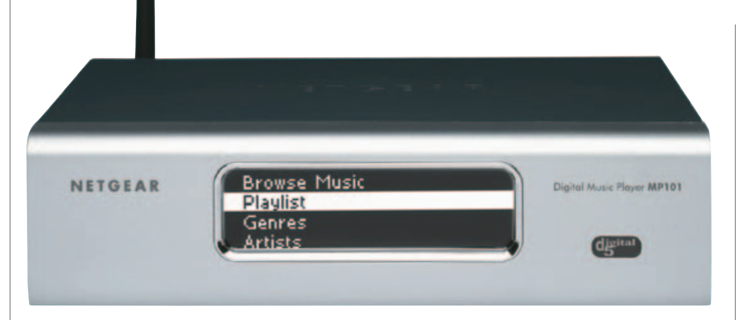
» Precio: 381 euros
» Web: www.audiotronics.es

VALORACIÓN

Funcionalidad de *streaming*, buena calidad de sonido, capacidad para cinco CDs y sintonizadora de radio. No es su especialidad, pero Philips hace notar su veteranía.

★★★★

Netgear MP101



Con el lanzamiento del nuevo MP101, los especialistas en redes de la empresa Netgear pretenden adentrarse en un mercado cuyas expectativas de crecimiento son muy grandes. Después de instalarlo y comprobar su funcionamiento, hemos observado algunos aspectos interesantes. El primero de ellos es la pantalla LCD de cuatro líneas. A través de ella podemos realizar búsquedas atendiendo a los artistas o nombre del grupo gracias al soporte para etiquetas inteligentes. Cuenta con mando a distancia que nos permite realizar todas las operaciones disponibles. También se incluye en el paquete de compra el software apropiado para reproducir listas bajo los formatos M3U, PLS y ASX. Cualquier lista de reproducción en estos formatos la podemos importar por medio de las aplicaciones WinAmp y Windows Media Player. En lo que respecta a las conexiones, cuenta con un amplificador de señal para las conexiones RCA, sin embargo se echa en falta alguna conexión digital. A diferencia de otros clientes de este tipo, el modelo que hemos analizado de Netgear cuenta con la posibilidad de encriptación de datos por medio del sistema WEP. Esta encriptación puede ser de 64 o 128 bits. Si tenemos un router conectado a la red, el cliente de Netgear no sólo reproduce los archivos de audio que nos proporciona el servidor, también es capaz de hacer *streaming* con las emisiones de radio a través de Internet. ■

CARACTERÍSTICAS

NETGEAR MP101

» Fabricante: Netgear
» Producto: MP101
» Formatos de audio: MP3, MP3pro, WMA
» Sintonizador de radio web
» Conexión de red: Ethernet y WLAN (54 Mbps)
» Salidas analógicas: Sí
» Salidas digitales: No
» Dimensiones: 240 x 67 x 185 mm

PRECIO Y CONTACTO

» Precio: 167 euros
» www.netgear.com

VALORACIÓN

Su precio más que asequible es uno de los principales valedores de este producto. Lejos de su terreno habitual, NetGear, sin embargo, nos presenta una solución sólida.

★★★★

Philips MX6000i

Los ingenieros y diseñadores de la compañía holandesa se ganaron el sueldo cuando decidieron fabricar este dispositivo. Por medio del MX6000i podemos reproducir DVDs, CDs, escuchar la radio ya sea de la forma convencional o vía Internet. A estas posibilidades hay que añadir la opción de reproducir fotos, vídeos e incluso un videojuego en nuestro PC y visualizarlo en la TV por medio de este producto de Philips. Se trata de una seria alternativa a los populares Media Center para lo que se ha denominado como entretenimiento digital en el hogar.

El dispositivo consiste en un reproductor de DVD con conector de red y un juego de altavoces *system surround*. El fabricante ha decidido integrar una sintonizadora de radio con funciones RDS y un cargador de cinco discos con soporte para DVD+R, -R, +RW, –RW y discos de doble capa. Respecto a los CDs, también soporta los formatos grabable y regrabable, incluidos aquellos que almacenen archivos en formato MP3.

Una vez lo hemos conectado y encendido, el dispositivo necesita al menos medio minuto para estar operativo. Durante este tiempo se comprueban las bandejas en las que se alojan los discos para «saber» si estamos trabajando con un CD o un DVD.

Además de las tradicionales conexiones de audio y vídeo, en la parte frontal encontramos una conexión de red Ethernet a 100 Mbps, lo que nos permite reproducir archivos de audio y vídeoque estén alojados en el disco duro de nuestro PC.

Basta con que arranquemos el gestor Media Manager de Philips, o cualquier otra aplicación UPnP que funcione como servidor. Los usuarios de Mac pueden descargarse de la web **www.streamium.com** un servidor compatible con esta plataforma. Con este software instalado, un Mac mini se convierte en un silencioso servidor para el MX6000i.

Otra de las posibilidades es trabajar de forma inalámbrica gracias a la controladora WLAN a 54 Mbps. Si no contásemos con controladora inalámbrica en nuestro PC, Philips nos proporciona un adaptador USB con capacidad para que podamos realizar *streaming* de vídeo en calidad MPEG-2.

Respecto a la reproducción de estaciones de radio *online*, podemos acceder a todas aquellas que están recogidas en la aplicación Shoutcast. Algunos juegos como el Tetris o el Solitario los podemos descargar directamente en el MX6000i y jugar con ellos visualizando las pantallas en la TV.

Todas las funciones están disponibles a través del mando a distancia, lo que nos hará la vida mucho más feliz a los que nos guste hacer todo desde el sofá. Respecto al panel frontal, encontramos los controles para realizar algunas funciones como el cambio de modo, de estación de radio, de tema en reproducción o de disco.

Los usuarios que estén pensando en adquirir una cadena de música pueden tener en este producto una alternativa muy seriapor varias razones. La primera y fundamental es que MX6000i cuenta con un amplificador que nos proporciona 75 watios por canal y sonido Dolby Digital, DTS o Dolby Pro Logic.

Aunque se trata de un sistema de sonido que no integra *subwoofer*, la reproducción de los sonidos graves se realiza a través de los frontales. Eso sí, éstos deberemos colocarlos a cierta distancia de la pared para que el sonido sea más claro y no se produzcan efectos desagradables, como vibraciones y eco.

En conjunto, este Philips MX6000i es un producto excelente. El precio puede parecer un poco elevado, pero lo cierto es que las características que ofrece abarcan casi todo el espectro del ocio. ■



CARACTERÍSTICAS

FABRICANTE: PHILIPS
PRODUCTO: MX6000I

- » Audio: MP3, MP3pro, WAV y WMA
- » Régimen de transferencia: 16-320 Kbpsw +VBR
- » Vídeo: MPEG1/2/4, DivX 3/5
- » Radio web: Sí
- » Amplificador: Sí. 6 x 75 watios
- » Ethernet: Sí
- » Wireless: Sí (54 Mbps)
- » UPnP: Sí
- » Salidas/Entradas analógicas: Sí/Sí
- » Entradas/Salidas digitales: Sí/Sí
- » Conectores vídeo: S-Vídeo, euroconector, vídeo compuesto.
- » Dimensiones: 240 x 67 x 185 mm

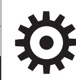
PRECIO Y CONTACTO

- » Precio: 771 euros
- » Web: www.streamium.com

VALORACIÓN

Sonido *surround*, reproducción de DVD y *streaming* por un precio razonable.

★★★★★



Pinnacle ShowCenter 200



Estamos ante la renovación de uno de los primeros clientes de vídeo que salieron al mercado de la mano de este fabricante. Un reproductor multimedia de nueva generación con el que la compañía consigue subirse al tren y se introduce en el estándar HD (alta definición) que permite reproducir tanto archivos de imágenes como de vídeo con una calidad inmejorable. Este estándar es capaz de reproducir vídeos con cualquiera de los formatos habituales como son WMV, AVI y MPEG, así como archivos de imágenes de alta resolución capturadas con cámaras de fotos digitales más avanzadas que pueden ser conectadas directamente al reproductor a través del puerto USB, que incorpora en su frontal.

Además de esta novedad principal se han mejorado aspectos de software de administración así como reproducción de radio a través de Internet. Se incluye una nueva aplicación que se instala en el ordenador que es capaz de gestionar los archivos que soporta el aparato para incluirlos en la base de datos compartida, a la que se conecta remotamente el reproductor. Esta base de datos genera colecciones de diferentes archivos para una localización más cómoda. La conexión se puede establecer mediante cable Ethernet o bien, si disponemos de un punto de acceso inalámbrico, por medio de su tarjeta de red inalámbrica que soporta el estándar 802.11b/g con antena direccional. Ello permite un acceso sin cables sin perjudicar en absoluto la reproducción, ya que el aparato obtiene el archivo tal cual aparece en la base de datos del ordenador, descodificándolo de forma local. El archivo se descomprime y se envía la información a la TV lo que permite una reproducción como si de un DVD se tratara, atendiendo siempre a la calidad del vídeo.

Por último, se ha pensado también en la grabación de vídeo en el PC. Si el ordenador dispone de una tarjeta PCTV, la función *timeshift* permitirá al usuario ver la TV, así como utilizar las opciones de reproducción de avance y retroceso a través de los programas en diferido. En efecto, se incluye un software de grabación en CD y DVD que permite crear y disfrutar vídeos y composiciones musicales profesionales creadas de forma casera.

Una de las funciones adicionales que sorprende agradablemente es el soporte UPnP, muy demandado por los usuarios y que permite disfrutar de servidores de *streaming* de otros fabricantes. ■



Pese a ser más pequeño que su antecesor, ofrece conectividad para cada necesidad.

CARACTERÍSTICAS

FABRICANTE: PINNACLE
PRODUCTO: SHOWCENTER 200

» Audio: MP3, WMA y WAV
» Transferencia: 16-320 Kbps +VBR
» Vídeo: MPEG-1/2/4, Divx 3/5, Xvid y WMV
» Amplificador: No
» Trabajo en red: Ethernet WLAN (54 Mbps)
» USB: Sí
» Salidas de vídeo: S-Vídeo, euroconector y vídeo por componentes

PRECIO Y CONTACTO

» Precio: 299 euros
» Web: www.pinnaclesys.com
» Teléfono: 91 395 63 60

VALORACIÓN

Dispositivo que nos ofrece todas las conexiones que pueda necesitar un usuario de a pie, lo que le hace interesante para aprovechar todos los aparatos del salón.

★★★★

Buffalo LinkTheater



A primera vista, el producto de este fabricante norteamericano parece un simple reproductor de DVDs. Sin embargo, en su interior podemos encontrar algunas características que lo diferencian claramente de estos productos. En primer lugar, cuenta con un disco duro en el que podemos grabar cualquier tipo de archivo de audio o vídeo. Además, posee una conexión Ethernet y WLAN, que podemos utilizar para acceder a contenidos de audio o vídeo proporcionados por un servidor. La interfaz de usuario es realmente sencilla, aunque la información de la reproducción de los archivos de audio es realmente pobre, ya que tan sólo se nos muestra aquella relativa a la canción en reproducción.

Si cuentas con un dispositivo para imágenes, ya sea un proyector o una pantalla de plasma, preparado para mostrar imágenes en alta definición, en este producto encontraremos un excelente aliado. En la parte posterior cuenta con una salida analógica de vídeo denominada YUV, que nos proporciona una calidad de imagen muy por encima del clásico euroconector. El cliente de *streaming* soporta vídeos en calidad HD, es decir, 1.080 píxeles de resolución horizontal entrelazada o 720 píxeles progresivos, aunque no es capaz de reproducir el formato HD DVD, dado que este sistema todavía no integra el gestor de derechos de autor, DRM.

Si contamos con un *router* con el que nos conectamos a Internet desde nuestra red doméstica, LinkTheater es capaz de reproducir vídeos y música obtenidos de Internet. Desafortunadamente, el reproductor soporta encriptación WEB pero WPA para las redes inalámbricas, lo que nos limita en algunas ocasiones la reproducción de archivos transferidos por vía inalámbrica.

Para mejorar la transmisión de datos a través de una red Wireless, los diseñadores de este producto le han dotado con dos antenas. Si, a pesar de esto, la conexión no es todo lo buena que deseáramos, cuenta también con un conector para una antena externa.

El fabricante nos ofrece también un servidor integrado. Aunque LinkTheater puede trabajar con un PC como si fuera un sistema de almacenamiento bajo el protocolo UPnP, su tamaño limita su capacidad de almacenamiento. A pesar de ello, integra un disco duro de 300 Gbytes, cantidad suficiente como para realizar labores de *streaming* de audio, pero a la hora de realizar la misma labor con archivos de vídeo, debemos revisar con asiduidad el espacio del que disponemos.

Si no estuviésemos satisfechos con las funciones estándar del servidor UPnP, podemos adquirir el software Oxilbox (**www.oxyl.de**) y probar con él. Esta alternativa para plataformas Linux y Windows extiende su funcionalidad por diferentes caminos.

Además de ver vídeos, reproducir música en diferentes formatos, escuchar la radio vía web o grabar la señal de TV, este Oxylbox nos permite navegar por Internet con algunas limitaciones, ya que no integra ActiveX ni Java.

Alternativamente, LinkTheater está preparado para mostrar los archivos almacenados en un dispositivo de almacenamiento externo gracias al puerto USB que encontramos en la parte frontal de este completo dispositivo. ■



Buffalo LinkTheater no sólo reproduce archivos del servidor: también puede leer dispositivos USB como las memory stick o discos duros externos.

CARACTERÍSTICAS

FABRICANTE: BUFFALO
PRODUCTO: LINKTHEATER

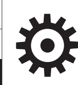
- » Audio: MP3, WAV, WMA y Ogg
- » Régimen de transferencia: 16-320 Kbps +VBR
- » Vídeo: MPEG, DivX 3/5, Xvid y WMV
- » Radio web: Sí
- » Amplificador: No
- » Ethernet: Sí
- » Wireless: Sí (54 Mbps)
- » UPnP: Sí
- » Entradas/Salidas analóg.: No/Sí
- » Entradas/Salidas digitales: No/Sí
- » Salidas de vídeo: S-Vídeo, euroconector y vídeo por componentes
- » Dimensiones: 420 x 50 x 265 mm

PRECIO Y CONTACTO

- » Precio: 279 euros (vía web)
- » Web: www.buffalo-technology.com

VALORACIÓN

Streaming integrado y puerto USB adicional. ★★★★★



Hauppauge MediaMVP

El cliente de *streaming* del fabricante francés lo podemos catalogar como uno de los primeros de su clase, gama de entrada. Por un precio asequible, la tarjeta MediaMVP nos permite ver vídeos, fotos o escuchar música en televisor sin que el PC esté presente. Gracias a sus múltiples menús, podremos seleccionar nuestros archivos favoritos gracias al mando a distancia. El PC funcionará como un servidor multimedia, distribuyendo a la MediaMVP los vídeos y medios seleccionados. Su compacto formato y su conexión Ethernet le ofrece un uso variado, sobre todo en la red ya que, si utiliza una MediaMVP con cada televisor y los conecta mediante un *hub* o *switch* Ethernet, toda la casa estará equipada para la reproducción de archivos multimedia. Esta tarjeta es muy fácil de instalar: basta con conectarla mediante el puerto Ethernet al ordenador y



utilizar el euroconector para conectar el PC al televisor.

El número de formatos soportados de forma nativa es algo limitado, MPEG1, MPEG2 y DivX.

En contraste, la interacción con otros productos de este fabricante es más que satisfactoria. Si el servidor está equipado con una sintonizadora de TV del mismo fabricante, el usuario de MediaMVP contará con un control absoluto sobre la grabación de las emisiones de TV. Desafortunadamente, no integra funciones de red y el análisis de la programación es algo obsoleto.

Si echamos un vistazo a la parte posterior observamos que las salidas son algo escasas, tan sólo integra un euroconector y conexión Ethernet. ■

CARACTERÍSTICAS

FABRICANTE: HAUPPAUGE
PRODUCTO: MEDIAMVP

- » Audio: MP3 y WAV
- » Régimen de transferencia: 16-320 Kbps +VBR
- » Vídeo: MPEG1, 2, 4, DivX y WMV
- » Radio web: Sí
- » Amplificador: No
- » Ethernet: Sí
- » Wireless: No
- » Salidas analógicas: Sí
- » Entradas analógicas: No
- » Euroconector: Sí
- » Dimensiones: 160 x 30 x 140 mm

PRECIO Y CONTACTO

- » Precio: 79 euros
- » Web: www.hauppauge.com

VALORACIÓN

Aunque con funciones muy básicas, la calidad de imagen es aceptable y su relación calidad-precio buena.

★★★★

Philips LCD TV 23IF9946

Del mismo modo que los productos de la serie Streamium, Philips se ha servido del estándar UPnP para integrarlo en esta pantalla LCD TV. Este aparato de TV LCD, además de las conexiones más comunes, cuenta con conexión de red y lógicamente con conexión VGA. Podemos reproducir en él, música, vídeos y fotografías proporcionados por un servidor, lo que le otorga a este dispositivo el primer puesto en lo que entretenimiento digital se refiere, ya que también esta preparado para recibir la señal de la televisión digital terrestre. También se proporciona con el paquete comercial un módulo para conexión WLAN.

En lo que se refiere al control remoto o mando a distancia, es compacto y completo. Permite realizar cualquier función aunque para acceder a alguna de ellas debamos pulsar varios botones, lo que hace que sea engorroso en ciertas situaciones.

Ese aparato de televisión cuenta con sonido *surround*, lo que nos proporciona una calidad de sonido respetable, más si lo comparamos con otros aparatos de TV cuyo sistema de sonido es de inferior calidad. Tan sólo dispone de una salida de audio a través de un *mini-jack*. Respecto a las conexiones de vídeo, se echa de menos una entrada DVI, lo que nos posibilitaría disfrutar de la resolución que nos ofrece la pantalla, 1.024 x 768 píxeles. Un buen complemento como segunda TV de la casa. ■



CARACTERÍSTICAS

FABRICANTE: PHILIPS
PRODUCTO: LCD TV 23IF9946

- » Audio: MP3, MP3pro, WAV
- » Régimen de transferencia: 16-320 Kbps +VBR
- » Vídeo: MPEG1, 2, DivX, Xvid
- » Radio web: Sí
- » Ethernet/WLAN: Sí/Sí
- » Entrada/Salida analógica: No/Sí
- » Entrada/Salida digital: No/No
- » Entrada vídeo: Euroconector, S-Video, YUV
- » Dimensiones: 690 x 455 x 247 mm

PRECIO Y CONTACTO

- » Precio: 1.499 euros
- » Web: www.audiotronics.es

VALORACIÓN

Televisión de 23 pulgadas con diseño elegante y soporte de *streaming*. No es suficiente para HDTV.

★★★★

Cómo administrar tus archivos multimedia con WMP 10

Para poder disfrutar de *streaming* desde un servidor UPnP resulta indispensable una base datos multimedia. Sólo de esta manera es fácil la búsqueda por artistas, canciones, álbumes o por géneros.

Windows Media Player no sólo reproduce cualquier contenido disponible, sino que está preparado para gestionar las etiquetas ID3 de los archivos MP3 y el mantenimiento de la base de datos. Además Windows Media Connect UPnP Server (WMC) accede directamente a dichas etiquetas ID3 y ofrece listas de canciones creadas con Media Player. Windows Media Connect está disponible para ser descargado gratuitamente desde **www.microsoft.com** o vía la función de actualización de Windows.

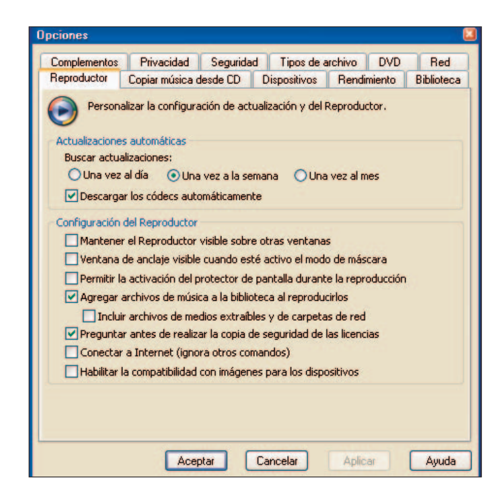
Con los siguientes ajustes de Media Player 10 puedes hacer que la gestión de archivos multimedia resulte muy simple. Si no deseas que cada archivo que se esté reproduciendo aparezca en la biblioteca de medios, deberás desactivar la correspondiente configuración en la pestaña *Reproductor* en *Herramientas/Opciones*.

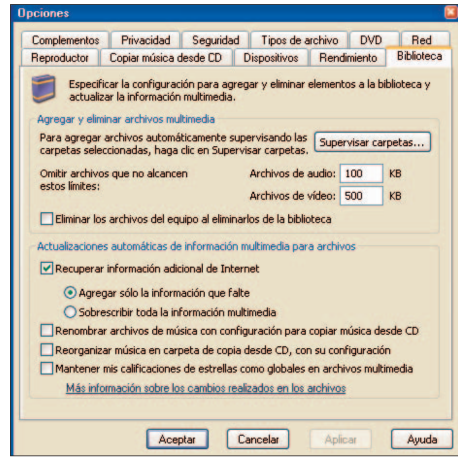
1 Supervisar carpetas

Selecciona la pestaña *Biblioteca multimedia* (todavía en *Opciones*). Aquí debes especificar, tras pulsar el botón *Supervisar carpetas*, qué carpetas deseas supervisar para encontrar archivos digitales nuevos, borrados, movidos o renombrados para actualizar la biblioteca multimedia según corresponda. Tan pronto como algún elemento de las carpetas cambia, las entradas correspondientes en la biblioteca de medios son automáticamente actualizadas.
Si dispones de conexión a Internet, Windows Media Player te servirá de gran ayuda en la gestión de etiquetas ID3 de una forma más eficaz que anteriormente. Simplemente activando la opción *Recuperar información adicional de Internet*, puedes especificar si la base de datos y las etiquetas de tus archivos de música serán dotados de información proveniente de las bases de datos de la Web. En estas bases de datos *on-line*, otros usuarios pueden haber añadido información que afecta a tus álbumes y canciones. Aquí deberás decidir si quieres añadir sólo la información adicional o si deseas sobrescribir toda la información recuperada.

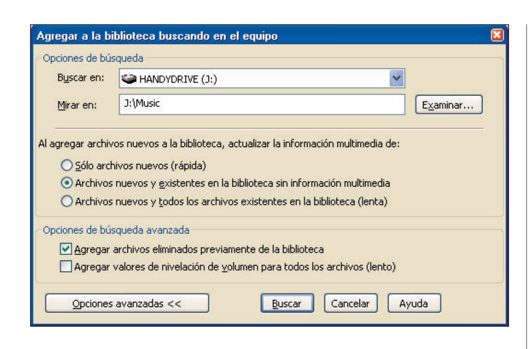
2 Limpiar la biblioteca

Si has activado todas las opciones, como paso siguiente tendrás que limpiar la biblioteca de

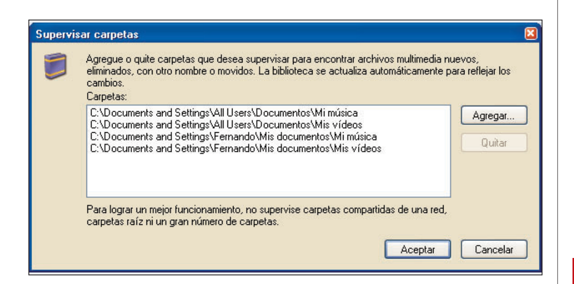




1 **WMP puede monitorizar carpetas y actualizar la biblioteca multimedia automáticamente.**



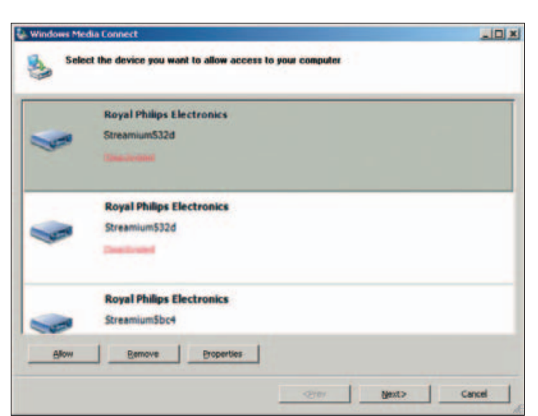
2 Es conveniente limpiar la biblioteca multimedia y posteriormente reconstruirla con los nuevos ajustes.



medios borrando las entradas y reconstruyéndolas. Cambia a *Biblioteca multimedia* (la cuarta opción de la izquierda). Selecciona todas las entradas de música y selecciona *Eliminar de la biblioteca* desde el menú contextual. Ahora presiona la tecla «F3» y especifica la carpeta (*Mirar en*) pulsando en *Examinar* para navegar por el disco y localizar el emplazamiento deseado. Media Player empieza inmediatamente a reconstruir la base de datos en función de los archivos que irá encontrando. Dependiendo del tamaño de tu colección, el proceso se tomará menor o mayor tiempo.

3 Ajustes básicos de WMC

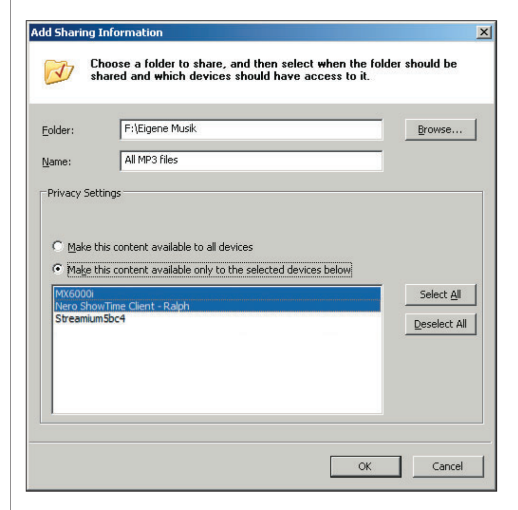
Si publicas tu colección multimedia con la ayuda de Microsoft UPnP server WMC, puedes configurar el servidor para su óptimo funcionamiento. Sólo se necesitan unos pocos pasos. Lanza la aplicación y haz clic en *Devices*. Selecciona *Add* para añadir los clientes UPnP que deseas que tengan garantizado el acceso a tu servidor. Verás una lista con cada cliente que está conectado a la red en ese momento. Selecciona cada cliente o sólo aquellos a los que deseas permitir el acceso y cierra la ventana pulsando sobre *OK*. Sólo los clientes que marcaste tendrán acceso a tus archivos multimedia.



3 Con WMC es posible mantener alejados a clientes no deseados. Sólo aquellos autorizados podrán acceder a tu biblioteca.

4 Archivos a compartir

Ahora tienes que determinar la compartición de contenidos. Presiona *Sharing* y haz clic en *Add*. Navega a través de tu sistema de archivos hasta alcanzar la carpeta donde tienes los vídeos, la música y las imágenes que quieres compartir. Puedes determinar si este contenido puede estar disponible para todos los clientes o sólo para ciertos clientes.



4 Existen diferentes derechos de acceso: puedes determinar qué clientes tienen acceso a todo el contenido.

GLOSARIO

STREAMING se refiere a una tecnología en la que el contenido es transferido a través de una red y reproducido mediante paquetes de datos que van llegando, en vez de esperar a que el archivo esté descargado por completo. Dadas las limitaciones del ancho de banda, el contenido multimedia ha de ser transmitido en formatos comprimidos como MP3, MPEG-1 o MPEG-2. Los clientes de *streaming* (software o hardware) trabajan por lo tanto con un *buffer* interno que les permite la reproducción pese a las alteraciones del canal emisor. Los clientes pueden manejar *streaming* de audio (MP3, WMA), vídeo (MPEG-1, 2 y 4, WMV, QuickTime) o de imagen (JPEG, PNG).

UPNP La mayoría del hardware de cliente para *streaming* soportan la tecnología UPnP (Universal Plug and Play). La arquitectura UPnP es una arquitectura de red distribuida y abierta que utiliza protocolos TCP/IP para permitir a los dispositivos conectarse sin trabas. Esto simplifica la implementación de redes. Los clientes de *streaming* que trabajan con TCP/IP pueden engancharse a una red y encontrar contenidos multimedia fácilmente. Estos clientes también pueden trabajar con diferentes servidores de aplicaciones. Puede tener sentido utilizar aplicaciones de otros proveedores para conseguir otras funcionalidades como por ejemplo controlar una tarjeta sintonizadora de televisión en un servidor PC.

RADIO INTERNET Las estaciones de radio de la Web utilizan tecnología de *streaming* para emitir sus contenidos. Ellas ofrecen tanto transmisiones en vivo como de material previamente grabado. La emisión suele realizarse en formato MP3 y puede reproducirse en programas cliente como WinAmp o con la mayoría de los clientes de hardware. La página www.shoutcast.com aloja miles de enlaces a emisoras web.

Preguntas y respuestas

¿Qué formatos de archivo y compresión son mejores para los clientes de *streaming*? ¿Es la conexión llamada Powerline Connection? Exponemos algunos de los problemas de *streaming* más habituales.



LinkStation de Buffalo es un dispositivo de almacenamiento externo que puede también utilizarse como servidor de *streaming*.

? Mis archivos MP3 varían en volumen. Ajustarlos manualmente es una ardua tarea. ¿Qué puedo hacer?

! Te aconsejamos utilizar la herramienta MP3Gain que se encuentra disponible en **mp3gain.sourceforge.net**. Esta herramienta analiza una o más canciones y a continuación normaliza cada una de las pistas.

? ¿Qué formatos de archivo y configuración de calidad es mejor para mi cliente de *streaming* de música?

! Normalmente, todos los clientes de *streaming* se reproducen comprimidos al igual que la música descomprimida. Un disco duro de 80 Gbytes almacena alrededor de 120 CDs de música descomprimida. En comparación, el formato MP3, a una tasa de bits de 192 Kbps, almacena 1.000 discos de audio. La opción 192 Kbps proporciona una excelente calidad así como un consumo inteligente del espacio en el disco. Incluso al nivel más alto (320 Kbps), podemos almacenar más de 400 CDs en un disco duro de 80 Gbytes.

? La aplicación servidor multimedia que incorpora mi cliente demanda demasiados recursos. ¿Hay alguna otra alternativa?

! Prueba con Twonkyvision (**www.twankyvision.com**), un software completamente gratuito. El servidor de música envía archivos de audio a la mayoría de los clientes de *streaming* más comunes. Otra posibilidad es versión del servidor multimedia (10 euros) que también envía datos de vídeo así como datos de imágenes. Ambos programas proporcionan las características de configuración a través de la interfaz web o la línea de comando. El servidor gratuito UpnP de Microsoft, Windows Media Connect, cuenta con algunas características especiales. Así por ejemplo podemos compartir archivos multimedia individualmente con los clientes de *streaming*. Asimismo, Windows Media Player cubre las funciones propias de administración de bases de datos.

? Cuento con un servidor de música Hermstedt Hifidelio. ¿Es posible suministrar música a otros clientes de *streaming*?

! Después de una actualización de software, la biblioteca de audio de Hifidelio debería estar disponible para cualquier otro cliente UpnP.

? ¿Hay alguna alternativa para utilizar redes con cable y redes inalámbricas?

! Sí, Powerline Connection (PLC). Con esta tecnología, una red se configura a través del circuito eléctrico de la casa. Los adaptadores parecen puntos de pared normales, pero el cableado suministra datos en vez de energía eléctrica. Como con las redes inalámbricas, la tasa de transferencia de datos aumenta con cada nueva generación. El sistema modernísimo Los últimos avances permiten alcanzar una velocidad computada de hasta 85 Mbps, aunque esta velocidad únicamente se alcanza bajo condiciones óptimas. Las interferencias serán causadas por las variaciones en la corriente de los distintos clientes. Si todo funciona bien, la tasa de datos de la tecnología Powerline Connection será suficiente para suministrar películas de calidad DVD a los clientes de *streaming*.

? Queremos renovar el sistema de cableado de nuestro chalet. ¿Deberíamos utilizar una red multimedia con cable?

! Si es posible técnicamente hablando es la mejor solución, ya que las redes inalámbricas son más vulnerables ante cualquier ataque además de ser menos fiables. También emiten ondas de radio continuamente, cuyos efectos pueden ser nocivos para la salud. Un cable convencional CAT7, por ejemplo, soporta conexiones de red rápidas a través de Gigabit LAN y proporciona seguridad adicional. Los cables de cada habitación tendrían que llevarse hasta un área central como puede ser el sótano. De este modo, el edificio siempre estará preparado para cualquier aplicación actual así como futuras aplicaciones, ya que este tipo de cableado puede también utilizarse para otras conexiones como el teléfono, RDSI o DSL.

OPTIMIZACIÓN



Antes nos conformábamos con que la red simplemente funcionara. En la actualidad la demanda ha crecido de forma exponencial y se exige que podamos enviar grandes cantidades de archivos de audio y vídeo de forma rápida por lo que las redes de alta velocidad resultan cruciales.



Mejorar la red es la historia interminable

Una cosa es conseguir que nuestra red sea operativa, y otra muy diferente es ajustarla para obtener el máximo rendimiento. Incluso aquellas que funcionan bien pueden ser mejorables.

En términos generales, no resulta muy difícil configurar una red basada en Windows para un entorno doméstico. Las tarjetas adaptadoras de red son reconocidas automáticamente e instaladas por Window XP. Las nuevas placas que integran el chip Gigabit Ethernet tampoco presentan grandes dificultades. Sus controladores se instalan durante la configuración inicial junto con los *drivers* para otros periféricos. Conecta tus equipos a un router de banda ancha con un servidor DHCP integrado, asigna las IPs y determina las carpetas a las que accederán, y ya está hecho.

Aunque esto resulta suficiente para cualquier usuario medio, aquellos fanáticos de la tecnología querrán optimizar la red tanto como sea posible. Y hay mucho margen para la mejora. La mayoría pensará que optimizar una red tiene que ver con mejorar la velocidad, pero existen otros aspectos. Por ejemplo, una red nunca es lo suficientemente segura. Sólo este punto es tan importante que hemos decidido abordarlos en un capítulo monográfico. La robustez de tu red es otra clave que tener en cuenta, evitando problemas de acceso a la red que suelen ser frecuentes.

Y EN CUANTO AL TRÁFICO DE DATOS, existen factores que son difíciles de ajustar pero que tienen un enorme impacto en el rendimiento de la red. Por ejemplo, piensa en tu conexión a Internet. Actualizar la velocidad de tu conexión te puede salir por 15 euros al mes, pero los beneficios que se obtienen son bien apreciables. Otro factor es el tipo de red que se utiliza. Seguramente cuentas con dispositivos Wi-Fi, pues resultan fáciles de instalar. En este caso alcanzarás una velocidad de transferencia de datos real de 2 o 3 Mbps y será muy complicado obtener ratios mayores. Si no te satisface, coge una taladradora y ponte manos a la obra para instalar el cableado Ethernet, y obtendrás un ratio de velocidad muchas veces superior al anterior, especialmente si utilizas una infraestructura de red Gigabit Ethernet. No es muy cara y resulta bastante sencilla de instalar. Sigue leyendo para saber qué equipamiento necesitas y que más tienes que tener en



Si el adaptador de LAN soporta 100 Mbps pero el cable sólo soporta 10, sólo podrás obtener 10 Mbps... la velocidad no puede ser mayor que la capacidad del cable.

“Una red puede ser siempre optimizada *a posteriori*”

cuenta. Las redes no necesitan tener un tráfico homogéneo. Mejora tu red integrando dispositivos inalámbricos o conexiones FireWire. Las redes FireWire ofrecen una alta transferencia de datos y se ponen en marcha casi de forma instantánea. Utiliza adaptadores especiales (*bridges*) de Windows XP para unir las diferentes redes en una sola, una red que esta medida para tus necesidades.

En contra de la opinión generalizada, las configuraciones por defecto de Windows para redes no son tan malas. Cierto es que algunos trucos o ajustes ocultos que hemos visto resultan insuficientes o, incluso peor, afectan negativamente en el rendimiento de la red. Sin embargo, existen algunas características que sí merece la pena cambiar. Muchas que vienen por defecto para entornos de oficina, pueden ser adaptadas para tu red doméstica. Encontrarás información en las siguientes páginas.

La línea de comandos típica de entornos operativos como DOS es una característica habitual de las herramientas de monitorización y optimización de la red. A aquellos usuarios más noveles, les instamos desde aquí que pierdan el miedo a trabajar con este tipo de líneas de comandos. De todas formas, en nuestras pistas y trucos hemos tenido en mente a aquellos que se resisten a trabajar con este tipo de herramientas para que echen por tierra el mito de las líneas de comandos.

HAY MUCHAS ÁREAS DE WINDOWS XP donde las características de red pueden ser configuradas. Dentro del *Panel de Control*, encontramos la opción *Conexiones de red*: aquí se gestionan todas las tareas de optimización y administración. En la zona de la izquierda se encuentra el enlace a las tareas más comunes como la creación de una conexión nueva. Todas las conexiones existentes se muestran en la parte de la derecha. Si seleccionamos una conexión concreta, a mano izquierda se muestran las tareas que se pueden activar para dicha conexión, como repararla o configurarla. Para configurar una conexión, haz doble clic sobre ella y nos aparece la ventana *Propiedades de Conexión de área local* y accederás al *Protocolo Internet TCP/IP*. Otra herramienta importante del Panel de Control es Windows Firewall. Aquí se configura el cortafuegos de Windows, que protege tu red pero que también puede dificultar la red si no está configurado adecuadamente.

Hay tareas de configuración avanzada que se incluyen en el epígrafe *Administración*, también dentro del Panel de Control. Se trata en realidad de una carpeta que permite la configuración de importantes servicios de red. Aquí se incluye la política de seguridad local, que ofrece importantes ajustes de seguridad. Y como siempre, contamos con el Editor de la Red (se activa siguiendo la ruta *Inicio/Ejecutar* y tecleando *cmd*) que nos da acceso a una línea de comandos donde realizar otro tipo de ajustes.

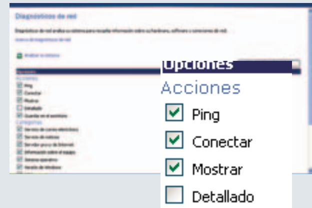
Además de las herramientas incluidas en XP, existe una amplia variedad de utilidades que te permitirán monitorizar y optimizar la instalación de tu red. En la sección *Utilidades/Red* de la página **www.download.com** encontrarás cientos de útiles herramientas, muchas de ellas gratuitas. La propia Microsoft ofrece numerosas utilidades de red. La más importante colección es Resource Kit. Para descargártelo ve a la página **http://go.microsoft.com/fwlink/?Linkid =4544** y a pesar de su nombre (Windows Server 2003 Resource Kit Tolls) muchos de estos programas de líneas de comando trabajan perfectamente con Windows XP. Después de instalártelo, encontrarás un archivo de texto que explica todas las herramientas incluidas.

INCLUSO SI TE ENCUENTRAS TOTALMENTE satisfecho con tu red, deberías echar un vistazo a este artículo. Quién sabe si en alguna de nuestras pistas, encuentras la solución a algún problema que te surgió y que dejaste aparcado por no encontrar su resolución.

Diagnósis rápida

1) **Selecciona *Inicio/Ejecutar*** y teclea CMD. Pulsa «Enter» y escribe *netsh diag gui* , y teclea «Enter» de nuevo. Se abrirá la herramienta de diagnóstico.

2) **En la ventana *Diagnóstico de red***, verás la tarea *Configurar las opciones de análisis* (debajo de



Analizar su sistema). Haz clic sobre ella y accederás a una nueva ventana donde se encuentra un largo número de opciones clasificadas en tres bloques: Internet, la información del equipo, los módems y los adaptadores de red,

3) **Ahora pulsa sobre *Analizar su sistema.*** El esca-



neado del sistema se llevará su tiempo.

4) **Finalmente, se muestran los resultados.** Haz clic sobre los campos que incluyen el símbolo + para expandir la entrada. Si aparece el mensaje *failed* en alguno de los campos, deberás subsanar la situación antes de proceder a la optimización de la red.





Si el adaptador de LAN soporta 100 Mbps pero el cable sólo soporta 10, sólo podrás obtener 10 Mbps... la velocidad no puede ser mayor que la capacidad del cable.

“Una red puede ser siempre optimizada *a posteriori*”

cuenta. Las redes no necesitan tener un tráfico homogéneo. Mejora tu red integrando dispositivos inalámbricos o conexiones FireWire. Las redes FireWire ofrecen una alta transferencia de datos y se ponen en marcha casi de forma instantánea. Utiliza adaptadores especiales (*bridges*) de Windows XP para unir las diferentes redes en una sola, una red que esta medida para tus necesidades.

En contra de la opinión generalizada, las configuraciones por defecto de Windows para redes no son tan malas. Cierto es que algunos trucos o ajustes ocultos que hemos visto resultan insuficientes o, incluso peor, afectan negativamente en el rendimiento de la red. Sin embargo, existen algunas características que sí merece la pena cambiar. Muchas que vienen por defecto para entornos de oficina, pueden ser adaptadas para tu red doméstica. Encontrarás información en las siguientes páginas.

La línea de comandos típica de entornos operativos como DOS es una característica habitual de las herramientas de monitorización y optimización de la red. A aquellos usuarios más noveles, les instamos desde aquí que pierdan el miedo a trabajar con este tipo de líneas de comandos. De todas formas, en nuestras pistas y trucos hemos tenido en mente a aquellos que se resisten a trabajar con este tipo de herramientas para que echen por tierra el mito de las líneas de comandos.

HAY MUCHAS ÁREAS DE WINDOWS XP donde las características de red pueden ser configuradas. Dentro del *Panel de Control*, encontramos la opción *Conexiones de red*: aquí se gestionan todas las tareas de optimización y administración. En la zona de la izquierda se encuentra el enlace a las tareas más comunes como la creación de una conexión nueva. Todas las conexiones existentes se muestran en la parte de la derecha. Si seleccionamos una conexión concreta, a mano izquierda se muestran las tareas que se pueden activar para dicha conexión, como repararla o configurarla. Para configurar una conexión, haz doble clic sobre ella y nos aparece la ventana *Propiedades de Conexión de área local* y accederás al *Protocolo Internet TCP/IP*. Otra herramienta importante del Panel de Control es Windows Firewall. Aquí se configura el cortafuegos de Windows, que protege tu red pero que también puede dificultar la red si no está configurado adecuadamente.

Hay tareas de configuración avanzada que se incluyen en el epígrafe *Administración*, también dentro del Panel de Control. Se trata en realidad de una carpeta que permite la configuración de importantes servicios de red. Aquí se incluye la política de seguridad local, que ofrece importantes ajustes de seguridad. Y como siempre, contamos con el Editor de la Red (se activa siguiendo la ruta *Inicio/Ejecutar* y tecleando *cmd*) que nos da acceso a una línea de comandos donde realizar otro tipo de ajustes.

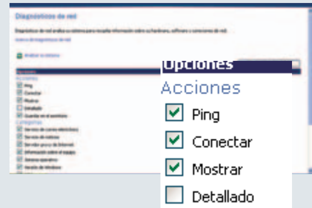
Además de las herramientas incluidas en XP, existe una amplia variedad de utilidades que te permitirán monitorizar y optimizar la instalación de tu red. En la sección *Utilidades/Red* de la página **www.download.com** encontrarás cientos de útiles herramientas, muchas de ellas gratuitas. La propia Microsoft ofrece numerosas utilidades de red. La más importante colección es Resource Kit. Para descargártelo ve a la página **http://go.microsoft.com/fwlink/?Linkid =4544** y a pesar de su nombre (Windows Server 2003 Resource Kit Tolls) muchos de estos programas de líneas de comando trabajan perfectamente con Windows XP. Después de instalártelo, encontrarás un archivo de texto que explica todas las herramientas incluidas.

INCLUSO SI TE ENCUENTRAS TOTALMENTE satisfecho con tu red, deberías echar un vistazo a este artículo. Quién sabe si en alguna de nuestras pistas, encuentras la solución a algún problema que te surgió y que dejaste aparcado por no encontrar su resolución.

Diagnósis rápida

1) **Selecciona *Inicio/Ejecutar*** y teclea CMD. Pulsa «Enter» y escribe *netsh diag gui* , y teclea «Enter» de nuevo. Se abrirá la herramienta de diagnóstico.

2) **En la ventana *Diagnóstico de red***, verás la tarea *Configurar las opciones de análisis* (debajo de



Analizar su sistema). Haz clic sobre ella y accederás a una nueva ventana donde se encuentra un largo número de opciones clasificadas en tres bloques: Internet, la información del equipo, los módems y los adaptadores de red,

3) **Ahora pulsa sobre *Analizar su sistema.*** El escaneado del sistema se llevará su tiempo.



4) **Finalmente, se muestran los resultados.** Haz clic sobre los campos que incluyen el símbolo + para expandir la entrada. Si aparece el mensaje *failed* en alguno de los campos, deberás subsanar la situación antes de proceder a la optimización de la red.





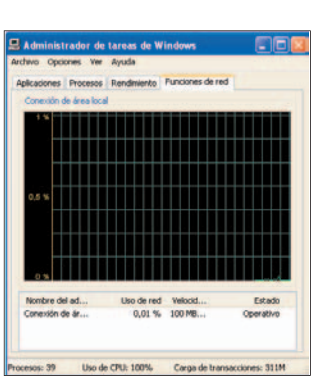
Conexiones más rápidas para audio y vídeo

Para disfrutar de todos los recursos de audio y vídeo no sólo necesitamos una conexión de banda ancha, sino que tendremos que optimizarla.

Control de red »

Administrador de tareas

Para detectar el efecto cuello de botella y acelerar nuestro sistema, hacemos uso del *Administrador de tareas* de modo que obtengamos información detallada sobre nuestra red. Presionamos las teclas «Ctrl + Alt + Supr». Resaltamos la pestaña la pestaña *Funciones de red* por lo que nos mostrará una representación gráfica de todas las conexiones de red, incluyendo las diferentes interfaces de red así como la velocidad máxima que soportan. En la pestaña *Ver* accedemos a la información sobre los *bytes* recibidos y enviados. Utilizamos las opciones de *Seleccionar columnas* para personalizar los datos que muestra la ventana principal.

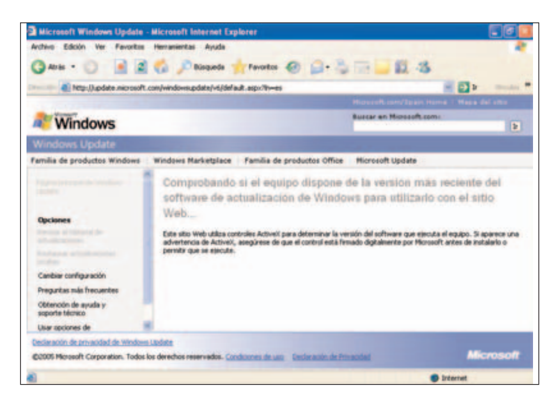


La pestaña *Funciones de red* del *Administrador de tareas* ofrece útiles opciones.

Controladores actualizados »

Windows Update

Los fabricantes de dispositivos de red ofrecen a través de sus páginas web los nuevos *drivers* disponibles para su descarga. Sin embargo, una mejor opción va a ser hacer uso de la utilidad *Windows Update*. Aquí Microsoft recoge los nuevos controladores, por lo que haciendo uso de esta utilidad estaremos absolutamente seguros de instalar el controlador correcto. Windows Update comprueba nuestro hardware y automáticamente consigue el *driver* adecuado, lo que evita cualquier búsqueda en la página web del fabricante del dispositivo. Además no surgirá ningún conflicto ya que todos lleva el certificado de XP. Abrimos Internet Explorer y vamos a la dirección http://windowsupdate.microsoft.com/. Seguimos las instrucciones de la pantalla, de modo que podamos instalar las últimas actualizaciones disponibles.



Mucho mejor que visitar la página web del fabricante de nuestro dispositivo de red, vamos al sitio de Microsoft que ofrece una navegación mucho más sencilla.

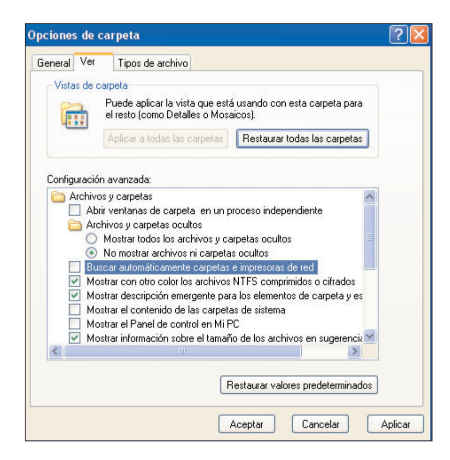
Acelerar nuestra red »

Gigabit Ethernet

La mayoría de las redes de hoy en día utilizan una velocidad de 100 Mbit/s. Esto se traduce en la salida máxima teórica de 12 Mbytes por segundo, aunque en la práctica este valor se ve restringido a más o menos la mitad. De todas formas, el cableado de la mayoría de las redes más modernas suele estar preparado para Gigabit Ethernet que nos permite superar esta velocidad (para estar seguros, comprobamos si disponemos de un cable *Cat 5e*). Sólo tenemos que reemplazar los adaptadores de red en cada uno de los ordenadores así como el *switch* que los conecta. Las tarjetas Gigabit Ethernet más baratas vienen a salir por unos 25 euros, y si disponemos de una ranura PCI no tendremos ningún problema para instalarla. Los *switches* Gigabit son algo más caros, unos 75 euros, y serán necesarios para conectar nuestro ordenador a velocidad Gigabit. Una vez instaladas las tarjetas de red y conectarlas al *switch*, deberíamos disfrutar de una red diez veces más rápida. De este modo, configurar una red Gigabit es uno de los mejores consejos que podemos dar.



Tendremos que desembolsar unos 25 euros por la tarjeta Gigabit Ethernet más económica. La velocidad que obtenemos no tendrá precio.



Ahorraremos bastante tiempo si deshabilitamos la opción *Buscar automáticamente carpetas e impresoras de red*.

Nada de búsquedas »

Ahorrar tiempo

Cuando reiniciamos nuestro ordenador, Windows comenzará a localizar las impresoras y carpetas compartidas. Si nuestro entorno cambia constantemente, podría ser muy útil, de otra manera sería una pérdida de tiempo. Para evitar todo este proceso, vamos a las *Opciones de carpeta* del *Panel de control* y resaltamos la pestaña *Ver*. Quitamos la marca de la casilla *Buscar automáticamente carpetas e impresoras de red*.

Asignar memoria a la tarjeta de red »

Mucha más capacidad

Asignar memoria a nuestra red de forma permanente es muy útil sobre todo para los ordenadores más antiguos. De este modo, la cantidad de RAM reservada no puede ser utilizada por nadie más. Para ello, determinamos el IRQ que nuestra tarjeta de red utiliza. Encontraremos que la información de la pestaña *Recursos* que encontraremos en la ventana de las propiedades de nuestra tarjeta de red, a la que accederemos a través del *Administrador de dispositivos*. Este *applet* se lanzará cuando presionemos la tecla de «Windows» y la tecla de «Pausa». Ahora abrimos el *system.ini* que localizamos en *C:\\Windows*. En la sección *386enh*, agregamos una entrada *Irq17=4096* donde reemplazamos el valor *17* por *Irq17* con nuestro actual número IRQ. Por último reiniciamos el ordenador.



Si tenemos dos redes distintas, podemos unirlas mediante una única conexión.

Conectar redes »

Puertos de red

Windows XP nos permite conectar distintas redes a través de un puerto. Imaginemos que tenemos una red Gigabit a través de cable, pero hay un ordenador que no puede integrarse ya que necesita conectarse a través de tecnología WiFi (podría ser un portátil que utilicemos en el jardín). En vez de comprar un equipo adicional, utilizamos uno de nuestros sobremesas como puente de modo que enlace la red WiFi con la red Gigabit Ethernet. Para establecer una red de este tipo, pinchamos en el icono *Conexiones de red* del *Panel de control*. Hacemos clic con el botón izquierdo del ratón sobre la primera conexión, mantenemos la tecla de «Ctrl» pulsada y hacemos clic con el botón izquierdo en la otra conexión. Ahora con el botón derecho del ratón pulsamos en cualquiera de las dos conexiones y elegimos la opción que nos permite establecer el puente. Ahora nuestro ordenador WiFi se encuentra completamente integrado en la red principal.

Visionar recursos compartidos de otras versiones »

Acceso más rápido

Si utilizamos un ordenador bajo Windows XP para acceder a los recursos compartidos de una máquina bajo Windows 98 o Me, experimentaremos una retraso significativo a la hora de visualizar los recursos compartidos. La razón de este comportamiento es que Windows XP está buscando tareas programadas en el otro ordenador. Para deshabilitar este proceso, pulsamos en *Inicio*, *Ejecutar* e introducimos *regedit* en la caja de texto que aparece. En el Editor del Registro, navegamos hasta *HKEY_LOCAL_MACHINE\Software\Microsoft\Windows\CurrentVersion\Explorer\RemoteComputer\NameSpace*. Marcamos la entrada *D6277990-4C6A-11CF-8D87-00AA0060F5BF*. Hacemos clic con el botón derecho del ratón y elegimos *Exportar*. Seleccionamos una localización y ahora eliminamos esa entrada. Reiniciamos el ordenador para que los cambios tengan efecto.

La búsqueda de recursos compartidos en ordenadores bajo versiones antiguas puede llevarnos bastante tiempo, por lo que cambiamos el Registro de Windows.

Comprobar nuestra conexión »

Comando ping

Si no conseguimos que un ordenador vea a otro, lanzamos una ventana de comando en ambos ordenadores. Introducimos *ipconfig* en la ventana *Ejecutar* para encontrar el número IP utilizado y darle el comando *PING 192.168.123.15*, donde el número indicado deber ser reemplazado por el número IP del ordenador remoto que estamos intentando contactar. Si no funcionara, es posible que tengamos un problema importante (hardware o *drivers*, por ejemplo) o bien que un firewall esté bloqueando la conexión. Si a pesar de todo seguimos teniendo problemas, tendremos que optimizar los recursos compartidos.



Xbox con Sharp en formato widescreen

La Xbox Microsoft trabaja de maravilla con tu TV

Cuidado con las configuraciones »

Parámetros de red

Los valores por defecto de algunos parámetros de red de Windows (RWIN y MTU) no son ideales para DSL ni para otros usuarios de banda ancha. La razón de que no sean perfectos para conexiones de banda ancha es que están diseñados para red. De este modo, si es más importante para nosotros las velocidad de transferencias de datos de nuestra rede doméstica que una aceleración de la navegación a través de Internet, entonces aconsejamos no jugar con los valores por defecto. Si lo hiciéramos, conseguiríamos lo peor de ambos lados.

Un servidor de impresión »

Impresoras

El modo más distinguido de imprimir en una red doméstica es utilizando una impresora que integre un servidor de impresión. Puede parecer algo exagerado, pero se trata únicamente de la conexión de nuestra impresora al *switch* a través de Ethernet. Asignamos un número IP fijo a nuestra impresora y utilizamos el protocolo IP. La configuración puede ser algo complicada, pero merece la pena. Así, allá donde agreguemos un nuevo ordenador a nuestra red, podremos imprimir en cuanto los *drivers* estén instalados… sin necesidad de cable.



No es necesario conectar la impresora directamente al ordenador. Los dispositivos con servidores de impresión integrados pueden utilizarse en cualquier red.

```
D:\WINDOWS\system32\cmd.exe
        Media State . . . . . . . . . . . : Media disconnected
        Description . . . . . . . . . . . : Bluetooth Device (Personal Area
rk)
        Physical Address. . . . . . . . . : 00-0B-6B-5A-37-DA

Ethernet adapter Local Area Connection:

        Connection-specific DNS Suffix  . :
        Description . . . . . . . . . . . : Broadcom 440x 10/100 Integrated
roller
        Physical Address. . . . . . . . . : 00-0A-E4-A4-B3-47
        Dhcp Enabled. . . . . . . . . . . : Yes
        Autoconfiguration Enabled . . . . : Yes
        IP Address. . . . . . . . . . . . : 192.168.178.21
        Subnet Mask . . . . . . . . . . . : 255.255.255.0
        Default Gateway . . . . . . . . . : 192.168.178.1
        DHCP Server . . . . . . . . . . . : 192.168.178.1
        DNS Servers . . . . . . . . . . . : 192.168.178.1
        Lease Obtained. . . . . . . . . . : Saturday, October 29, 2005 7:09:
M
        Lease Expires . . . . . . . . . . : Tuesday, November 08, 2005 7:09:
M
```

Una útil herramienta para comprobar nuestras conexiones de red es el comando *ipconfig/all*.

Comprobar nuestra configuración »

Línea de comandos

Una línea de comandos es la forma más eficiente de diagnosticar cualquier problema de red. Para lanzar una línea de comando, pinchamos en *Inicio*, *Ejecutar* e introducimos *cmd* en la caja de texto. Ahora tecleamos *ipconfig/all*. Nuestro ordenador visualizará una lista con todos los adaptadores de red, incluyendo información detallada sobre todo lo que necesitamos si surgiera algún problema o cuando intentamos optimizar nuestra red.

Visionar recursos compartidos »

Localizar más rápido en la red

Acceder a los elementos compartidos de otro ordenador, llevará un tiempo hasta que todos ellos aparezcan listados. Afortunadamente, existe una forma de acelerar este proceso. Pinchamos en *Inicio*, *Ejecutar* e introducimos *regedit* en la caja de texto. En el Editor del Registro navegamos a *HKEY_LOCAL_MACHINE\SYSTEM\Current ControlSet\Services\LanmanServer\Parameters*. Creamos un nuevo valor *dword* que llamaremos *SizReqBuf* y configuraremos a 14596 (decimal). Una vez reiniciado el ordenador, los recursos compartidos estarán visibles más rápidamente.

Optimizar y reparar problemas con Live CD »

Live CD

Incluso si no somos usuarios de Linux, este sistema operativo gratuito puede ofrecernos grandes ventajas. No es necesario tener Linux instalado en nuestro disco duro, ya que hay versiones que pueden arrancarse desde un CD-ROM o DVD-ROM como por ejemplo Suse Live, Knoppix, Kanotix e Insert. Estos CDs incluyen *drivers* para los dispositivos más importantes, por lo que normalmente tenemos acceso directo a la red con tan sólo reiniciar desde el CD. Así la utilización de un Live CD es la forma más rápida y sencilla de solucionar cualquier problema si sospechamos que los dispositivos de hardware o cableado puedan ser la causa. Si nuestra red funciona bajo Linux, el inconveniente no estará en el hardware. Si no fuera así, buscamos el dispositivo que provoca el problema en vez de perder el tiempo intentando arreglar los *drivers* de Windows.

Revisar nuestras conexiones »

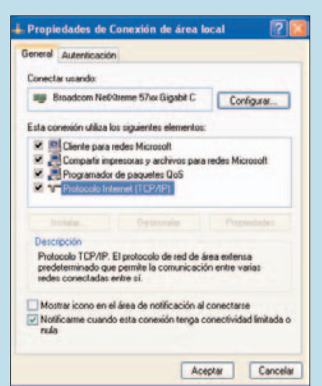
Netstat

Si sospechamos que alguna de las conexiones que disponemos no se ha establecido correctamente, hacemos uso del comando NETSTAT. Así, nos mostrará una útil estadística de todas las conexiones tanto a nivel de red local como a nivel de Internet.

Utilizar redes FireWire »

FireWire

Existe una manera de configurar rápidamente una sencilla pero a la vez rápida red. Así, utilizamos las características de red FireWire integradas en Windows XP. Una red FireWire es muy rápida y se comporta del mismo modo que una red Ethernet. Sin embargo, no es posible conectar un *switch* utilizando una red FireWire, ya que ésta es únicamente para unir dos ordenadores. En las *Conexiones de red* del *Panel de control*, encontraremos la conexión 1394. Accedemos a sus propiedades, hacemos doble clic sobre el protocolo IP y utilizamos la dirección IP *192.168.123.1*. Asignamos *192.168.123.2* a otro ordenador y configuramos la máscara de subred a *255.255.255.0* en ambas máquinas. Ahora nuestra red FireWire está preparada para funcionar.



FireWire es uno de los mejores modos para enlazar dos ordenadores.

La conexión más rápida posible »

El chip correcto

La velocidad teórica de Gigabit Ethernet es más o menos igual a la de PCI bus. Si el dispositivo Gigabit Ethernet se conecta a través de tecnología PCI al ordenador, algo que ocurre en la mayoría de las tarjetas de expansión de hoy en día, no puede conseguir la máxima velocidad. Afortunadamente, muchos chipset actuales utilizan tecnologías especiales para conectar un chip Gigabit y traspasar el cuello de botella producido en el PCI. El problema es que los fabricantes de placas base suelen agregar un Gigabit secundario en su placa. Estos chips secundarios no utilizan la conexión directa y además ofrecen transferencias mucho más lentas, por lo que en ocasiones provocan algún que otro problema. De este modo, si la placa base ofrece más de una conexión Gigabit Ethernet, siempre utilizamos la nativa al chipset, no la secundaria.



PREGUNTAS Y RESPUESTAS

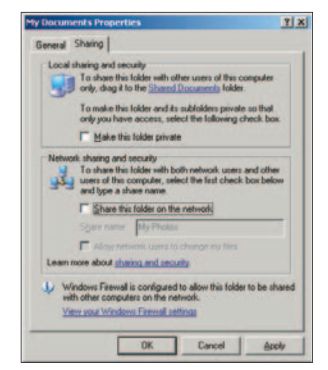
En casos aislados una red rápida verá como cae su velocidad a la del dispositivo más lento dada la mezcla existente de cables, hardware y software. Se trata del típico cuello de botella.

? Debido a un ataque de virus, perdí una partición entera. Y como si esto no fuera suficiente, ahora tengo problemas con mi entorno de red. La partición perdida alojaba una carpeta compartida (*E:\Fotos*). He creado una nueva partición *E:* y dentro una carpeta con el nombre *Fotos*. Windows XP la reconoce como compartida, pero no funciona como tal. ¿Qué puedo hacer?

! Windows XP piensa que todavía reconoce la carpeta compartida pero está «equivocado». Tienes que «descompartir» la carpeta y luego volver a compartirla para que las cosas empiecen a funcionar. Haz clic sobre el directorio compartido con el botón derecho del ratón y en el menú emergente selecciona la opción *Compartir y seguridad*. Copia el nombre de tu carpeta compartida al Portapapeles («Ctrl + C»). Ahora deshabilita el campo *Compartir esta carpeta con la red* y presiona *Aceptar*. Abre otra vez la caja de diálogo y haz un tic en *Compartir esta carpeta con la red*. Inserta («Ctr + V») el nombre antiguo de la carpeta y pulsa *Aceptar*. Tu carpeta ya deberá funcionar apropiadamente.

? He oído que las redes FireWire son rápidas de instalar, y que puedo obtener altas tasas de transferencia de datos. Sin embargo, mi PC de sobremesa todavía utiliza Windows 2000 y no deseo cambiarlo ya que me funciona perfectamente; y ciertamente me da miedo que se estropeen las cosas. Ahora bien, si conecto mi portátil via FireWire a mi PC Windows 2000, este último busca un Microsoft 1394 PC y pregunta por los controladores. ¿Dónde puedo conseguir dichos controladores?

! Por desgracia, sólo Windows XP (y el denostado Windows Me) son capaces de funcionar en redes FireWire sin necesidad de software de terceros. Pero existe una programa shareware llamado FireNet que puede ayudarte. Lo encontrarás en **www.unibrain.com/evaluations/firenet.htm**, desde donde puedes bajarte una versión de prueba. Sólo se mantiene activo durante media hora pero no tiene limitaciones de funcionalidad. Basta con reiniciar el equipo para contar con otros 30 minutos gratis. Te puedes registrar para la versión completa por 30 dólares, pero por ese precio mejor es que adquieras una tarjetas Gigabit Ethernet.



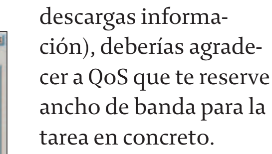
Algunas veces es más fácil chequear activar y desactivar la opción de compartir en la Red para resolver los problemas de reconocimiento de carpetas.

? Me gustaría actualizar mi red doméstica a Gibabit Ethernet. Sin embargo, hay algunas cuestiones que todavía me preocupan. Con un dispositivo más lento, como mi impresora de red que utiliza una tarjeta estándar 100/10, ¿la red se va a ver ralentizada? Mi router de banda ancha incluye un conmutador 100/10: ¿puedo seguir utilizándolo? El ordenador de mi hija, basado en un Celeron 800 (data del año 2001) ¿ganará con Gigabit Ethernet?

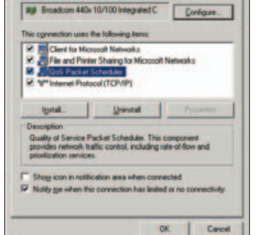
! Primero de todo, necesitarás un *switch* Gigabit Ethernet. Estos conmutadores incluyen normalmente el código 10/100/1000, y esto significa que saben automáticamente cómo gestionar los equipos de estas tres diferentes velocidades sin que se reduzca el rendimiento de los dispositivos. De esta manera tu impresora de red no obstaculizará al sistema ni tampoco tu router de banda ancha, pero asegúrate de no conectar ningún dispositivo Gigabyte directamente al router. Mejor conéctalos sobre el Gigabyte para que se puedan comunicar a alta velocidad. Conecta tu puerto *uplink* del *switch* al router de banda ancha y no utilices los puertos del router salvo para dispositivos lentos como tu impresora. Y efectivamente, incluso con viejos ordenadores, experimentarás una mayor velocidad de transferencia de datos.

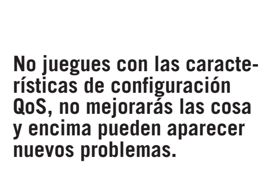
? Me han comentado que puedo aumentar la velocidad de mi red limitando el servicio QoS (Quality of Service). Este servicio toma el 20 por ciento de la memoria disponible en el ancho de banda que utiliza para realizar ciertas funciones de control. Esta cantidad puede ser reducida a cero, ¿es verdad?

! No. Esta creencia generalizada es definitivamente incierta. QoS no consume parte de tu ancho de banda. En todo caso, permite que las aplicaciones aprovechen el ancho de banda. De esta manera, mientras no hay aplicaciones ejecutándose en tu sistema, no habrá consumo del ancho de banda. Por otro lado, si necesitas aplicaciones que necesitan un espacio del ancho de banda (por ejemplo llamadas por Voz IP que no se interrumpan cuando te

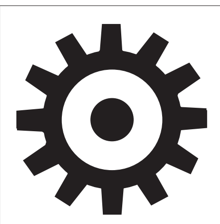


descargas información), deberías agradecer a QoS que te reserve ancho de banda para la tarea en concreto.





No juegues con las características de configuración QoS, no mejorarás las cosa y encima pueden aparecer nuevos problemas.



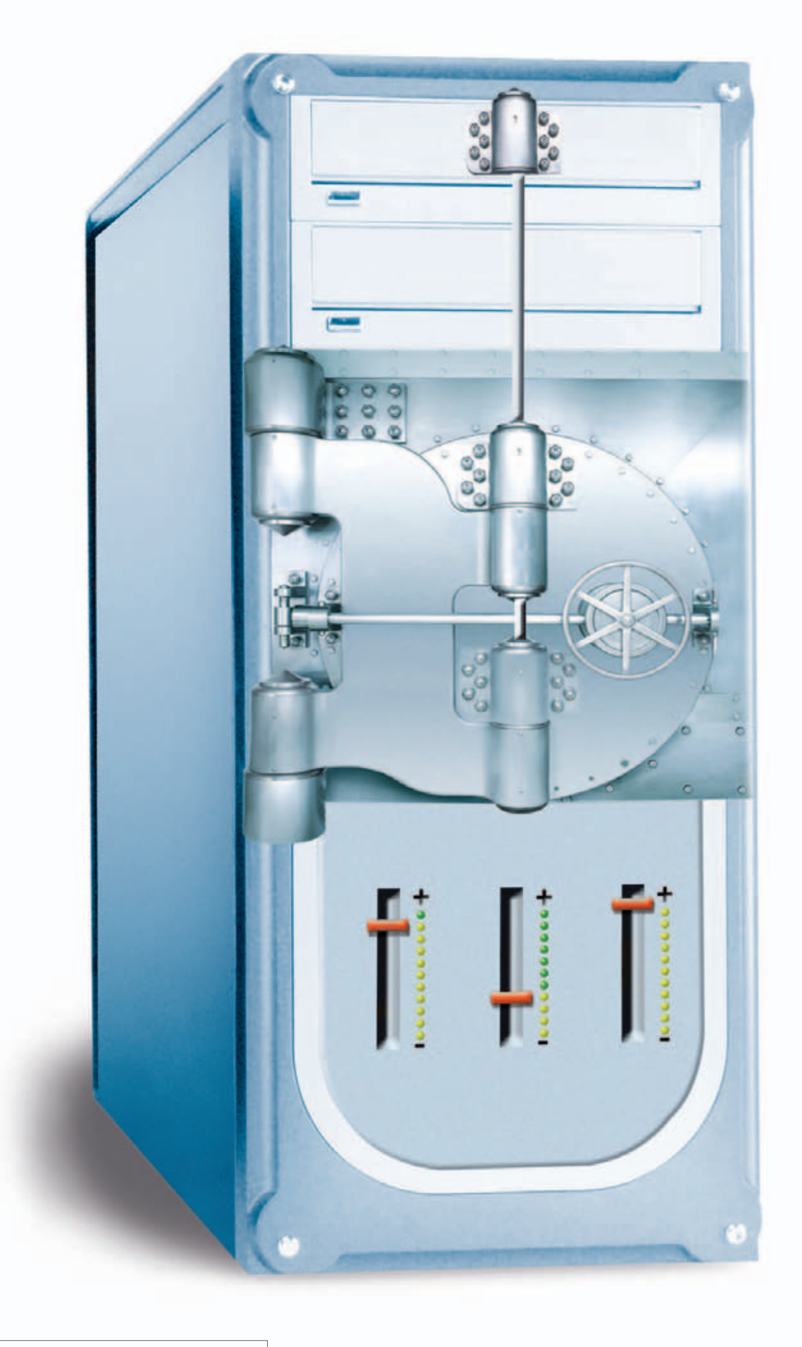
PROTECCIÓN



¿Pagar por proteger tu sistema? Si no lo haces, lo pagarás caro. A continuación, echa un vistazo a la siguiente guía de seguridad que te proponemos.

No pierdas tiempo... blinda tu ordenador

Microsoft sigue lanzando diferentes campañas de seguridad y, aun así, los PCs con Windows siguen considerándose inseguros. ¿Son acaso víctimas de una prensa injusta?



Ningún PC es una isla. Las amenazas a las que tiene que hacer frente un ordenador dan la sensación de estar a la vuelta de la esquina. Así, los virus y gusanos se cuelan en nuestro correo electrónico; el *spyware* consigue ocultarse hábilmente en herramientas que resultan prácticas y útiles; los *hackers* y troyanos se hacen con un hueco dentro de nuestro sistema y los espías profesionales vigilan los correos y archivos de nuestro portátil, equipo de sobremesa o red. No podemos hablar de un cien por cien de seguridad en nuestra máquina a no ser que adoptemos una postura extrema: nada de *e-mails*, Internet, disquetes o CDs que nos deje algún amigo o familiar. Pero como todos sabemos, esto no es factible y resulta prácticamente imposible llevarlo a la práctica.

Windows se ha convertido en el objetivo favorito que todos aquellos que desarrollan y distribuyen cualquier tipo de código malicioso. Hay herramientas específicas que permiten desarrollar virus de forma casi automática.

Existe un número de determinados agujeros dentro de nuestro sistema operativo y demás aplicaciones que muchos usuarios no se molestan en solucionar, cuando la instalación de las últimas actualizaciones de seguridad ofrecidas por Microsoft bastaría para resolver nuestros problemas. Dado que existen millones de equipos que tienen como sistema operativo Windows, los fabricantes de virus no se van a molestar en atacar un sistema operativo diferente.

EXISTE UN NÚMERO DETERMINADO DE PCS CON WINDOWS que no cuentan con la protección suficiente para hacer frente al *malware*. La solución que requerirá este tipo de máquinas pasa por un antivirus que rastrea cada uno de los archivos y correos electrónicos que provienen de Internet o un disco, por ejemplo. Esta especie de guardián tiene que estar actualizado para ser capaz de reconocer los virus más recientes, troyanos o gusanos. Incluso, si no te puedes permitir productos comerciales como Norton Antivirus o Trend Micro PC-Cillin, tienes a tu disposición diversas herramientas antivirus gratis que te resultarán



Consigue protección para que Windows sea tan seguro como cualquier otro entorno de trabajo.

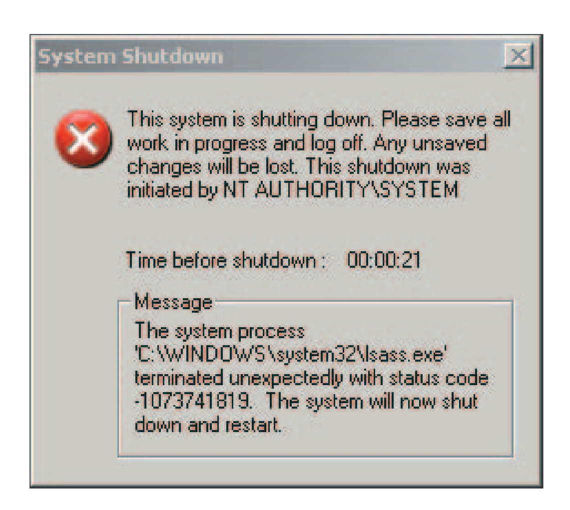
"Las amenazas para tu PC están en cada curva"

de gran utilidad. Bitdefender y AVG, por ejemplo, ofrecen una versión de sus productos sin gasto alguno para el bolsillo (siempre y cuando no hagamos de éstas un uso comercial). Por esta razón, no existe ningún motivo para no proteger tu ordenador frente al ataque de cualquier tipo de *malware*.

Cuando un PC o una red está conectada permanentemente a Internet, nos exponemos a que los intrusos intenten hacerse un hueco a través de varios puertos (éstos están reservados para HTTP, FTP y otro tipo de tráfico) para conseguir acceder a nuestra máquina. Si conectamos una red entera a Internet, colocaremos normalmente un *router* entre la red en cuestión y el mundo que hay a su alrededor. La mayoría de estos *routers* tienen integrado un firewall, que es el que va a proteger la pasarela (*gateway*) entre nuestra red privada e Internet. Para configurar un firewall, el administrador, en primer lugar, deshabilitará todos los puertos (algunos firewalls vienen con todos los puertos desactivados, de todas maneras), permitiendo exclusivamente los que son necesarios. Si no tienes un firewall físico, deberías instalarte un software (firewall personal o de escritorio) para permitir el tráfico de aquello que quieres dejar pasar. Un firewall personal no sólo monitoriza el tráfico entrante, sino que también se encarga del tráfico saliente, bloqueando todo elemento que resulte sospechoso, como el software espía. Aquí, tienes la posibilidad de escoger entre productos comerciales como Norton Personal Firewall y herramientas gratuitas como Zone Alarm.



Si el *Escritorio* de Windows te lanza mensajes de error inesperados es hora de buscar los motivos. A menudo es un virus el que nos engaña y no una función específica, programa especial o algún elemento del hardware. Lo primero de todo será echar mano de un antivirus antes de «buscar culpables».

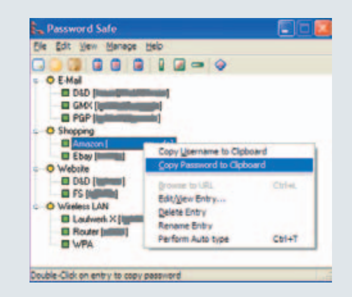


CUANDO ENVÍAS MENSAJES Y DOCUMENTOS a través del correo electrónico, tienes que tener presente que éstos pueden ser interceptados y leídos por otras personas. Para asegurar su confidencialidad, tendrás que encriptarlos antes de hacerlos llegar a su destinatario. La encriptación de archivos y carpetas es también una vía de protección para la información almacenada en el disco duro de nuestro ordenador. Antes, hemos mencionado que Windows, por su diseño, es inseguro. Después de su instalación, este sistema operativo se ejecuta bajo el modo administrador, lo que significa que el usuario tiene todos los privilegios sobre su sistema, haciendo también labores de intrusismo. En otras palabras, cuando ejecutas Windows utilizando la cuenta del Administrador, los virus, troyanos, programas espía y *hackers* que usurpan el control de tu PC tienen los mismos privilegios administrativos que tú. ¿Por qué sucede esto? La respuesta la encontramos en el hecho de que otros sistemas operativos como Linux se suelen ejecutar en una cuenta con privilegios limitados. En Windows es posible configurar e sistema de tal manera que puedas trabajar con una cuenta que tenga limitada sus derechos, conectándonos como administrador cuando realmente necesitemos privilegios como tal.

Contraseñas seguras

1. Usa ocho o más caracteres.
2. Combina caracteres numéricos, de tipo especial, además de las mayúsculas y minúsculas.
3. No emplees palabras de tu entorno personal (por ejemplo el nombre de tu mejor amigo o tu mascota).
4. Desecha las palabras que pueden encontrarse en un diccionario (los *hackers* usan los ataques a los directorios para quebrantar contraseñas).
5. Evita fechas como las referidas a los cumpleaños.
6. Simplemente no añadas caracteres especiales o numéricos a las palabras. Intégralos.
7. No escribas al revés palabras que puedan encajar en alguna de las categorías.
8. Si tienes que escribir tu contraseña pero piensas que puedes olvidarla, anótala en un papel, pero no la coloques en un lugar visible.
9. Echa mano de distintas contraseñas para cada sistema (correo, encriptación, compras *on-line*, etc).
10. Nunca reveles tu contraseña.

Para crear una contraseña que nadie pueda averiguar, prueba a pensar en una secuencia en la que además de letras mayúsculas y minúsculas, des cabida a otro tipo de elementos como números y signos de puntuación. A continuación, emplea la primera inicial de cada uno de los términos que conforman la frase que has pensado para obtener tu contraseña. Recurre a herramientas del tipo Password Safe, de Bruce Scheiner (http://passwordsafe.sourceforge.net) para elaborar y proteger una base de datos que contenga tus contraseñas.



Almacena tus contraseñas en una herramienta segura como Password Safe.

Elementos imprescindibles para redes rápidas y fiables

Parte de la popularidad de Windows XP se debe a su facilidad de uso con conexiones LAN. Aunque este es un entorno muy goloso para cualquier *malware*.

Chequea tu firewall »

Atelier Web Firewall Tester

El hecho de que se haya instalado un firewall no significa necesariamente que el sistema sea seguro. La máquina puede estar todavía abierta. Para localizar los agujeros en cada uno de los apartados, utilizamos una herramienta como Atelier Web Firewall Tester (AWFT) o un escáner *on-line* (ver el cuadro de la derecha). Podemos adquirir AWFT por 20 dólares, una copia gratuita para su evaluación realizará diez pruebas y ejecutará otras distintas en el firewall. AWFT lleva a cabo seis test que, de acuerdo con el fabricante, ninguno de los firewall más populares pasa sin revelar cierta debilidad. Y esto fue probado en nuestro banco de pruebas.



Atelier Web Firewall Tester detectó seis agujeros de seguridad en las configuraciones del Firewall de nuestra máquina.

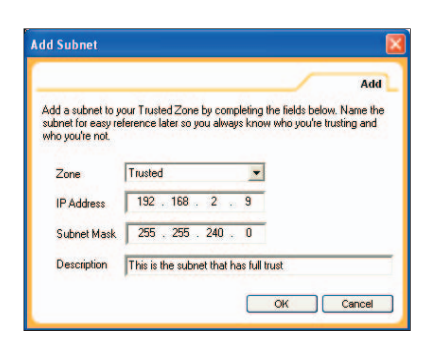


El escáner *on-line* de Sygate no ha localizado ningún problema... tampoco lo ha hecho el servicio de Symantec. De este modo, nuestro sistema está perfectamente guardado por el firewall.

Escáneres on-line »

Symantec, Sygate

Symantec y Sygate ofrecen escáneres gratuitos que comprueban los puertos de nuestro sistema a través de Internet. Vamos a http://security.symantec.com/sscv6 y a http://scan.sygate.com, respectivamente, y tendremos nuestro sistema completamente chequeado. Symantec requiere Internet Explorer 5 o una versión superior e instala un control ActiveX, mientras que Sygate acepta otros navegadores.
Si disponemos de un firewall configurado correctamente, como parte de un router LAN inalámbrico o un módem DSL combo, no tiene por qué haber problemas.



Zone Alarm nos permite agregar ordenadores y redes a el área *Trusted Zone*.

Direcciones seguras »

Zone Alarm

Zone Alarm nos permite agregar direcciones de servidores y ordenadores a una zona bajo el nombre *Trusted Zone*. Esta área normalmente cuenta con configuraciones menos restrictivas si la comparamos con el área normal que lleva el título de *Internet Zone*. Para agregar un ordenador o una red a *Trusted Zone*, pinchamos en el enlace del *Firewall* (a la izquierda) y resaltamos la pestaña *Zones*. Hacemos clic en el botón *Add* y seleccionamos el tipo de dirección que queremos agregar. Ahora introducimos todos los detalles y pinchamos en *OK*.

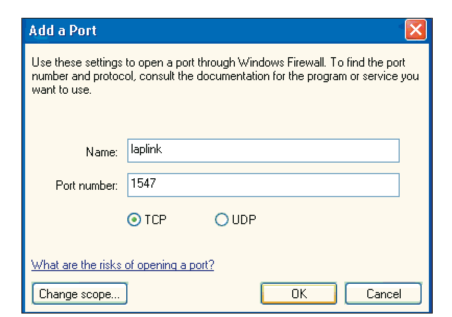


Zone Alarm protege nuestra bandeja de entrada de códigos VBS.

Mensajes seguros »

Zone Alarm

Zone Alarm protege nuestra entrada de correo de códigos maliciosos VB Script. En el panel izquierdo, seleccionamos *Email Protection*. Configuramos la opción *Basic Mailsafe Settings* a *On*.



Es posible configurar el Firewall de Windows para Laplink.

Configurar el Firewall de Windows para Laplink »

Windows XP

Para configurar el Firewall de Windows que incluye el Service Pack 2 de XP, abrimos el firewall en el Panel de control (*Inicio/Panel de control/Firewall de Windows*). Resaltamos la pestaña *Excepciones* y pinchamos en el botón *Agregar programa*. Seleccionamos *Laplink* de la lista de programas (o pinchamos en el botón *Examinar* si no estuviera). En la pestaña *Excepciones*, pinchamos en el botón *Agregar puerto*. Tecleamos Laplink 1547 como puerto y número de puerto. Nos aseguramos que la opción *TCP* está seleccionada y pulsamos en *Aceptar*.

Cerrar automáticamente el ordenador cuando no se usa »

Zone Alarm

A menudo dejamos desatendido nuestro ordenador durante un largo periodo de tiempo, pero no nos desconectamos. Deberíamos entonces desactivar el acceso a Internet en Zone Alarm. Lanzamos Zone Alarm, seleccionamos *Program Control* en el panel a mano izquierda y configuramos la opción *Automatic Lock* como *On*. Pinchamos en el botón *Custom*. Configuramos el temporizador, estipulando los minutos de inactividad que estará. Por último seleccionamos *Block all internet access*.



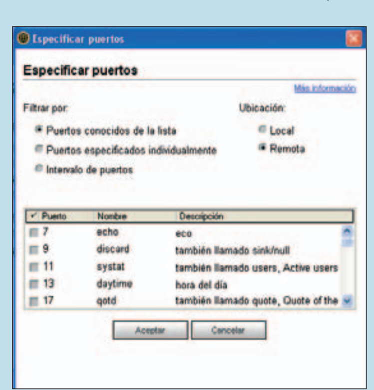
Configuramos Zone Alarm para cerrar nuestro ordenador si no estamos frente nuestro Escritorio.

Permitir conexiones Laplink »

Norton Personal Firewall

Para permitir las conexiones remotas a través de Laplink en un sistema protegido por Norton Personal Firewall, será necesario configurar nuestro firewall. Seleccionamos *Configurar*, resaltamos la pestaña *Programas* y pinchamos en el botón *Agregar*. Abrimos la carpeta *Laplink* instalada por defecto en *C:\Archivos de programa\Laplink Gold*, seleccionamos el icono *laplink.exe* y pinchamos en *Abrir*. Ahora resaltamos la pestaña *Avanzado* y pinchamos en el botón *General*. Pulsamos en el botón *Agregar* y nos aseguramos de que la opción *Permitir* se encuentra seleccionada para a continuación pinchar en *Siguiente*. Seleccionamos *Conexiones con y desde otros equipos* y hacemos clic en *Siguiente*. Elegimos *Cualquier equipo* y volvemos a pulsar en *Siguiente*. Seleccionamos TCP como protocolo y a continuación *Sólo los tipos de comunicación o puertos que se enumeran a continuación*. Hacemos clic en *Agregar* y elegimos *Puertos especificados individualmente*. Tecleamos 1547 como número de puerto y hacemos clic en *Aceptar* y luego en *Siguiente*. En caso de que queramos registrar una entrada para que se cree cada vez que una conexión Laplink se realiza, creamos una entrada y hacemos clic en *Siguiente*. Ahora seguimos las instrucciones de la pantalla hasta finalizar el proceso.

Para casos especiales, como permitir acceso remoto desde Laplink, debemos definir una nueva regla en Norton Personal Firewall.



Especificamos el puerto a través de la conexión remota.

Activar Alerta de ataques »

Norton Internet Security

Una de las nuevas características de la edición 2005 de las herramientas de seguridad de Norton es la Alerta de ataques. Si disponemos de una conexión permanente a Internet, *Alerta de ataques* consigue información en tiempo real sobre las últimas amenazas de Internet. Tan pronto como se detecte una nueva amenaza, nos informa sobre ella y lo que debemos hacer si considera que nuestra sistema no está protegido. Si disponemos de la edición 2005 ó 2006 de las herramientas de seguridad de Symantec, aconsejamos activar la alerta en el Centro de Seguridad de Internet. También nos aseguramos de que en la caja de diálogo *Opciones* se encuentren activadas las opciones *Activar LiveUpdate automático* y *Comprobar si hay actualizaciones para Detección de intrusiones* (ambas están en la pestaña *LiveUpdate*).

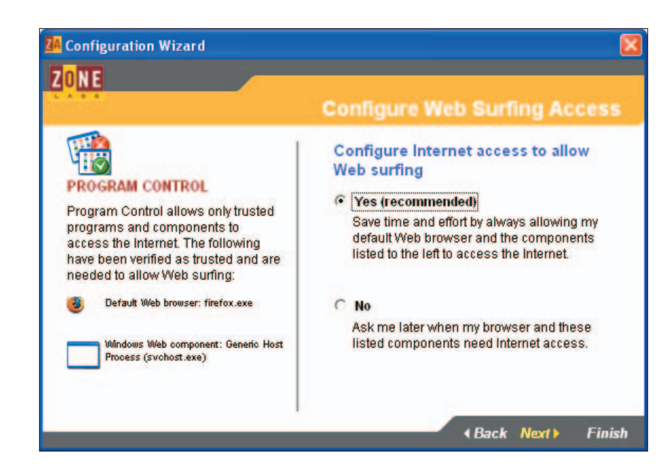


Activamos *Outbreak Alert* para proteger nuestro sistema de las últimas amenazas.

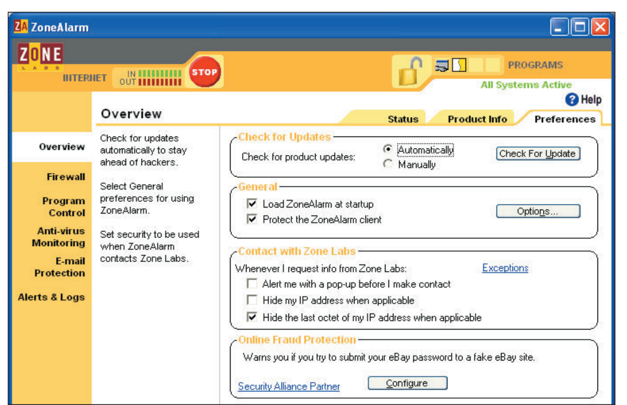


Configura tu propio firewall

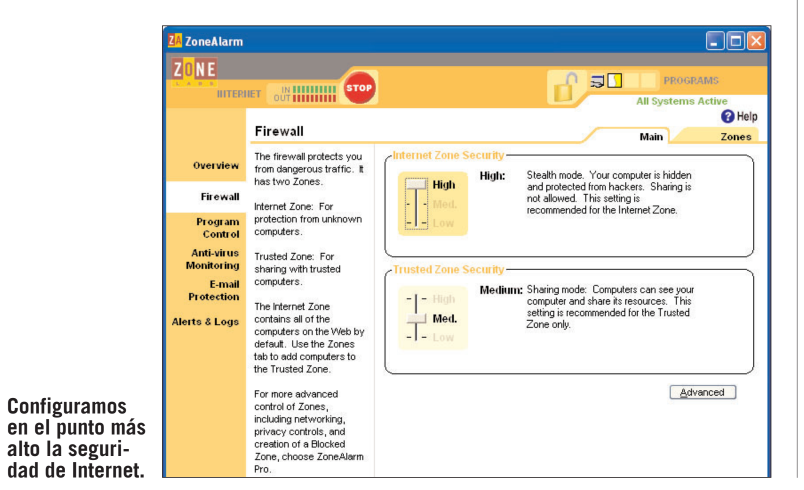
A menos que nos desconectemos de la Red, no disfrutaremos de una protección completa. Además de las herramientas antivirus y las aplicaciones *antispyware*, un cortafuegos es indispensable en un ordenador bajo Windows que además disponga de una conexión a Internet. La mayoría de los usuarios confían en el firewall integrado en Windows XP, aunque los más exigentes que requieren una mejor protección y un mayor control sobre su sistema harán uso de un firewall más potente como el que incluye Zone Alarm o Norton Personal Firewall. Mostramos en las siguientes páginas la forma de configurar el cortafuegos de Zone Alarm así como las configuraciones más importantes de la propuesta comercial de Norton.



1 Dejamos que Zone Alarm configure automáticamente nuestras aplicaciones de Internet.



2 Zone Alarm conseguirá actualizaciones automáticas de su página web.



3 Configuramos en el punto más alto la seguridad de Internet.

1 Instalación de Zone Alarm

Descargamos la edición gratuita de Zone Alarm de la dirección www.zonealarm.com e instalamos el software. Seguimos las instrucciones del asistente para configurar Zone Alarm. Dejamos que la herramienta automáticamente configure el acceso a Internet para nuestro/s explorardor/es. Pinchamos en *Done* y reiniciamos el ordenador.

2 Selección de preferencias

Resaltamos la pestaña Preferences y activamos la casilla Check for product updates automatically. Configuramos Zone Alarm para cargarse desde el menú de Inicio y protegemos el cliente Zone Alarm.

3 Configuramos la seguridad del firewall

Para configurar una contraseña, pinchamos en el botón Configure bajo la opción Online Fraud Protection. Pulsamos en el botón Add, introducimos la contraseña dos veces y pinchamos en OK también por partida doble. En el panel izquierdo seleccionamos Firewall. Movemos la barra de desplazamiento Internet Zone Security hasta High. Establecemos en Medium la zona Trusted Zone Security, que contiene las configuraciones de nuestra red. Es posible agregar otros ordenadores o redes a través de la pestaña Zones.

4 Programas de control

Seleccionamos Program Control en el panel izquierdo y resaltamos la pestaña Programs. Aquí Zone Alarm lista todas las aplicaciones que requieren acceso a Internet así como los permisos que tienen cada una de ellas. Desde aquí podemos



4 Seleccionamos nuestras aplicaciones para permitir o bloquear el acceso a Internet.



5 Elegimos si permitimos o denegamos a una aplicación los derechos de acceso una vez o cada vez que lo intente.

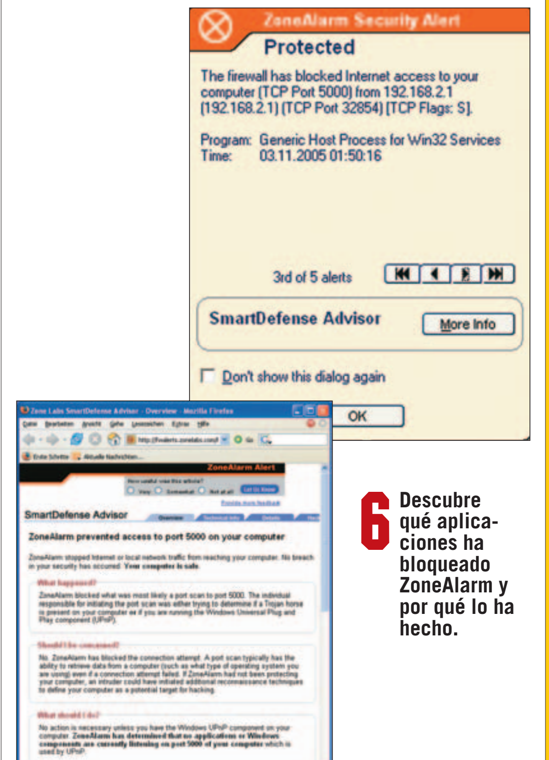
cambiar las configuraciones, haciendo clic en el símbolo junto a cada aplicación y seleccionando Allow, Block o Ask. Cuando queremos agregar un programa a la lista, pinchamos en el botón Add situado en la parte inferior de la caja de diálogo. Seleccionamos el archivo «.exe» y luego configuramos los permisos de acceso.

5 Permitir o denegar el acceso

Cuando iniciamos una aplicación que no está listada en la lista de Zone Alarm, pero que intenta acceder a Internet, Zone Alarm nos avisará de que el archivo .exe solicita acceso a Internet. Si queremos permitir un acceso permanente a Internet de la aplicación o simplemente queremos bloquearlo, activamos la opción Remember this setting y pinchamos en el botón Allow o Deny. Para deshacer la acción Remember this setting, vamos a la lista Program Control (ver Paso 4) y cambiamos las configuraciones para la aplicación.

6 Comprobar las alertas de seguridad

Zone Alarm una vez activo bloqueará una serie de intentos de acceso a Internet. Normalmente, aparecerá una caja de diálogo que nos avisará del número de alertas. Navegamos a través de ellas pinchando en los botones en forma de flecha en la caja de diálogo. Si queremos que nos informe sobre una alerta en particular, pulsamos en el botón More info del campo Smart Defense Advisor. Con esto lanzamos nuestro explorador de web y se abrirá una página de ayuda en el sitio web de Zone Alarm. Podemos observar durante un tiempo que cada vez que intenta el acceso es bloqueado y comprobamos si es necesario realizar algún tipo de acción. Cuando estemos seguros de que no hay peligro, marcamos la opción Don´t show this dialog again y cerramos la alerta de seguridad. Ahora estamos protegidos, por lo que nuestro ordenador estará seguro.



6 Descubre qué aplicaciones ha bloqueado ZoneAlarm y por qué lo ha hecho.

Norton Personal Firewall

Si utilizamos un Firewall de otro fabricante como puede ser Norton Personal Firewall, también es posible configurarlo.

Norton Personal Firewall es uno de los componentes del paquete Norton Internet Security. Pinchamos en el enlace *Firewall personal* de la ventana *Estado del sistema* y hacemos clic en el botón *Configurar* situado a la derecha.

En la pestaña *Firewall*, activamos *Activar Firewall personal* y seleccionamos el nivel de seguridad *Supervisor*. Pinchamos en el botón *Personalizar nivel* para asegurarnos de que todas las configuraciones son correctas. Configuramos el Firewall a *Alto*. Desactivamos los controles ActiveX y Java.

En la pestaña *Programas*, seleccionamos la opción *Activar Control de programa automático*. Todas las aplicaciones que han solicitado acceso a Internet aparecerán listadas en la parte inferior de la caja de diálogo. Podemos cambiar la configuración para cada programa, seleccionamos las distintas opciones.



Asegúrate de que el firewall de Norton está configurado como *Alto*.

¿Seguro que eso es un virus?

Visionar películas o escuchar radio a través de Internet son acciones que nos exponen a diferentes peligros. Hay un malware **especializado en cada tipo de aplicación.**

Qué hacer en caso de emergencia »

Todos los antivirus

Nuestro PC se comporta de una forma extraña por lo que sospechamos que está infectado por un virus, gusano o troyano. ¿Qué podemos hacer?

1. La mayoría de ellos pueden eliminarse fácilmente. El procedimiento suele ser reinstalar Windows así como las distintas aplicaciones y datos. Es importante realizar las copias de seguridad oportunas.
2. Detener la conexión a Internet. Muchos virus, gusanos y troyanos utilizan Internet para extenderse. Desconectamos el módem, el adaptador RDSI o el módem DSL.
3. Cerramos el ordenador utilizando *Inicio/Apagar*. Si Windows no responde, apagamos directamente el ordenador.
4. Reiniciamos el PC utilizando el disco de arranque de emergencia. Los paquetes antivirus suelen ir provistos de un disco de arranque que inicia el ordenador en el modo DOS y lanza su escáner en busca de virus.
5. Eliminamos el *malware* y tomamos nota del virus que ha infectado nuestro ordenador.
6. Reiniciamos Windows y nos descargamos un antivirus actualizado de la página web del fabricante. Pasamos un escáner completo a nuestro ordenador y eliminamos cualquier *malware*. Si esto no funcionara, hacemos uso de una de las alternativas *on-line* disponibles.
7. Visitamos las páginas web de las compañías desarrolladoras de software antivirus, para así averiguar algo más sobre el virus en cuestión. Quizá todavía quede algún agujero en cuestiones de seguridad. Si fuera así, instalamos las actualizaciones de seguridad que ofrece Microsoft.

En la página web de Symantec encontramos más información sobre el virus que ha infectado nuestra máquina.



Utilizamos BartPE para crear un disco de arranque.

Crear un disco de arranque »

Windows

Si el software antivirus no incluye un disco de arranque, es posible crear uno. Así dispondremos de una herramienta que nos ayudará a extraer los archivos que necesitamos para el disco de arranque del CD de instalación de Windows. Podemos encontrar todas las instrucciones para crear un disco de arranque en la página de Lagerweij.

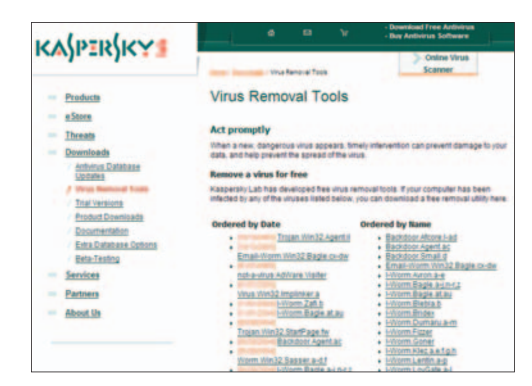
www.nu2.un/pebuilder

Usar un antivirus *on-line* »

Trend Micro y Kaspersky

Es algo arriesgado ejecutar un ordenador bajo Windows sin una protección antivirus actualizada. Sin embargo, puede haber casos en los que un escáner antivirus no funcione debido a una infección seria. En esos casos, hacemos uso de un antivirus *on-line* capaz de localizar este mal. Las compañías antivirus como Trend Micro y Kaspersky ofrecen servicios *on-line* que nos permiten chequear nuestro PC a través de Internet. Vamos a **http://es.trendmicro-europe.com** o **www.kaspersky.com** para acceder a este tipo de servicios. También es posible enviar un archivo infectado a los laboratorios de Kaspersky para que nos facilite toda la información pertinente.

Si no disponemos de ninguna protección antivirus en nuestro ordenador, Trend Micro ofrece una sección bajo el nombre de *House Call* que chequea *on-lin*



Karspersky, Grisoft y Bitdefender ofrecen herramientas para eliminar virus específicos.

Hacer uso de un escáner especializado »

Kaspersky, Grisoft, Bitdefender

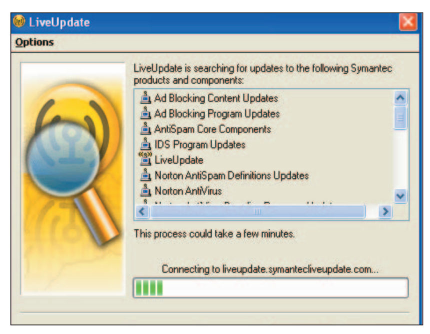
Muchas veces somos conscientes del virus o gusano que ha instalado en nuestro sistema, ya que uno de nuestros contactos nos comunica que su ordenador lo ha enviado a todas las entradas de su libreta de direcciones. Los especialistas antivirus como Kaspersky, Grisoft y Bitdefender ofrecen herramientas que toman medidas específicas contra virus, gusanos o troyanos particulares. Vamos a **www.kaspersky.com/removaltools** o nos dirigimos a la página de descargas de **www.grisoft.com** o **www.bitdefender.com** y seleccionamos la herramienta antivirus correspondiente: *Virus Removal Tools*. Nos descargamos la herramienta y la utilizamos para eliminar el *malware*. Incluso así, deberíamos pasar un escáner completo de nuestro sistema una vez el malware se ha eliminado.

Actualizar las definiciones de virus »

Todos los antivirus

Antes de escanear nuestro sistema en busca de un código malicioso, comprobaremos que están actualizadas las últimas definiciones de virus en la página web del fabricante. De este modo, nos aseguramos de que el escáner reconoce las últimas amenazas.

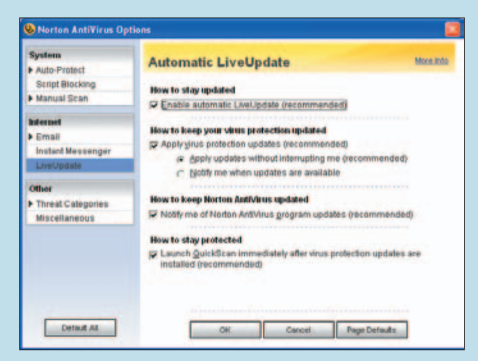
Actualizamos las definiciones de virus de nuestro software antes de pasar el escáner antivirus.



Actualizaciones automáticas »

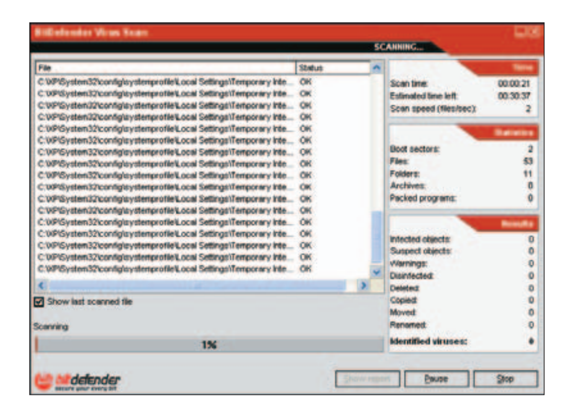
Todos los antivirus

Muchos antivirus se configuran con frecuencia casi diaria para conseguir actualizaciones así como las últimas definiciones de virus.



Configuramos Norton Antivirus para instalar automáticamente *LiveUpdate*.

Para deshabilitar las actualizaciones automáticas en Symantec Norton Antivirus, por ejemplo, lanzamos el programa y pinchamos en el botón *Opciones*. En el panel de mano izquierda seleccionamos *LiveUpdate* y activamos *Aplicar las actualizaciones de protección contra virus (recomendado)* y *Aplicar las actualizaciones sin interrumpir*. También recomendamos pedirle al programa que nos notifique sobre las actualizaciones disponibles. Si contamos con una copia de Norton Internet Security, deberíamos también activar las actualizaciones automáticas para todas las aplicaciones de Norton. Así seleccionamos *Opciones* y pinchamos en *LiveUpdate*. Aquí activamos *Activar LiveUpdate (automático)*.



Bitdefender Free Edition comprueba los archivos y carpetas a demanda, nunca se ejecuta en el fondo.

Evitar conflictos entre antivirus »

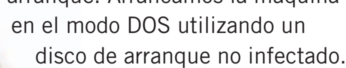
Todos los antivirus

Los distintos antivirus del mercado obtienen distintas puntuaciones en los diferentes apartados, sobresaliendo cada uno de ellos en una sección específica. ¿Sería una acertada decisión instalar más de un antivirus para que vele por una apartado en particular? La respuesta es no. Los programas antivirus son herramientas que suelen ejecutarse en el fondo chequeando los nuevos archivos y mensajes. Al instalar dos programas del mismo tipo, nuestro sistema puede colgarse o bien que una aplicación invalide a la otra. Lo mejor que podemos hacer es instalar un paquete completo, como Norton Antivirus, y utilizar un segundo escáner pero evitando que éste último se ejecute en el fondo. De este modo podremos comprobar un archivo sospechoso utilizando varios escáneres. Una combinación que trabaja a la perfección es Antivir Personal Edition (**www.free-av.com**) junto con Bitdefender Free Edition (**www.bitdefender.com**). Antivir PE cuenta con un escáner a tiempo real que se ejecuta en el fondo, mientras que Bitdefender Free Edition ejecuta únicamente su escáner si el usuario así lo requiere.

Disco de arranque maestro »

Windows

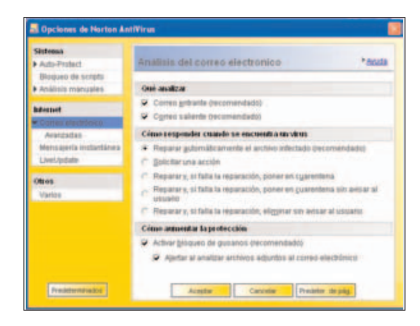
Si un virus ha infectado el disco de arranque master (MBR/Master Boot Record) de nuestro disco duro, intentamos eliminarlo utilizando nuestro software antivirus. Si no fuera posible, será necesario volver a grabar este disco de arranque. Arrancamos la máquina en el modo DOS utilizando un disco de arranque no infectado. Ejecutamos el comando *fdisk/mbr*. Con ello conseguimos crear un nuevo disco de arranque maestro, eliminando el virus sin causar ningún daño a la instalación de Windows. Aun así, antes de nada, realizamos una copia de seguridad de cualquier documento importante.



Chequeo de mensajes »

Todos los antivirus

Gran parte del *malware* viene a través de mensajes de correo, por lo que es importante que nuestro antivirus esté configurado para comprobar automáticamente nuestros mensajes de correo electrónico. En Norton Antivirus abrimos el panel dedicado al correo electrónico en las *Opciones de Norton Antivirus* y activamos *Correo entrante (recomendado)* y *Correo saliente (recomendado)*. Comprobamos que esté activada la casilla *Activar bloqueo de gusanos (recomendado)*. Si por algún motivo desactivamos estos análisis automáticos, nos aseguramos de no abrir los archivos que recibamos por e-mail, si antes no los hemos comprobado manualmente.

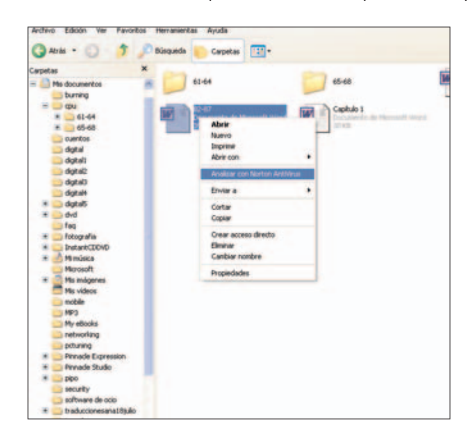


Es aconsejable disponer de un análisis automático que compruebe nuestros mensajes.

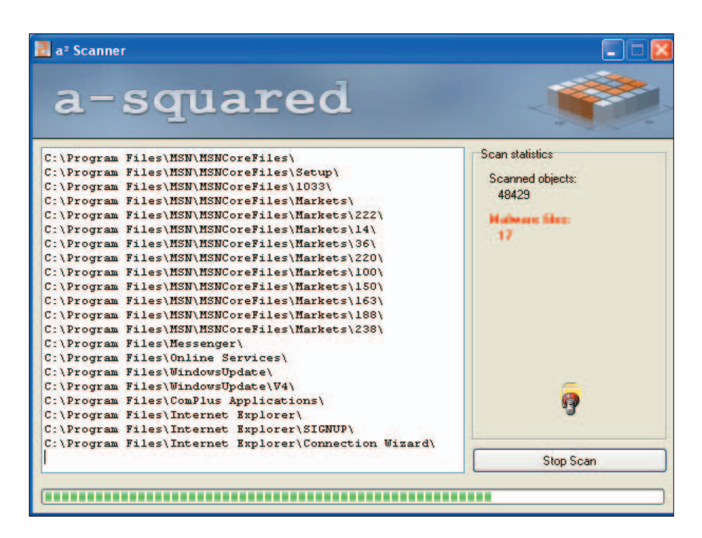
Escaneo rápido de un archivo »

Todos los antivirus

Cuando recibimos un archivo a través de correo electrónico que sospechamos que contiene cualquier *malware*, guardamos éste en el disco duro. Lanzamos el Explorador de Windows y hacemos clic con el botón derecho del ratón en el archivo. La mayoría de los antivirus agregan una opción al menú de contexto, de modo que podemos comprobar si el archivo está infectado con tan sólo pulsarla. Es posible realizar este mismo proceso con carpetas completas.



La mayoría de los antivirus incluyen una opción en el menú de contexto que nos permite escanear archivos y carpetas.



A2 Free sirve de complemento a nuestro antivirus y es capaz de localizar troyanos, *dialers* y *spyware*.

Desafiar a un troyano »

A2 Free

No todos los paquetes antivirus ofrecen la protección adecuada contra troyanos, *dialers* y *spyware*. Si nuestro firewall nos notifica la presencia de troyanos como *Subseven* o *Netbus*, quizá el software antivirus haya sido engañado. Aquí es donde entra en juego una herramienta gratuita como A2 Free de **www.emisoft.com/en/software/free** (o su equivalente comercial A2 Personal Edition). Instalamos la herramienta y escaneamos la carpeta (o el disco duro completo) en busca del *malware*.

Proteger el sector de arranque »

Windows

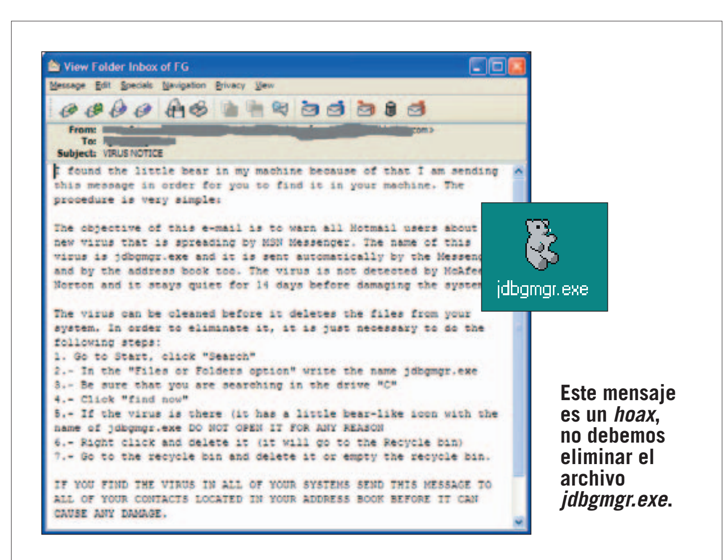
Los virus del sector de arranque contagian el disco duro al arrancar el PC con el disco infectado insertado en la unidad correspondiente. Para evitar esto, deberíamos configurar la BIOS de la máquina de modo que ignore cualquier disquete que se encuentre en su unidad. Reiniciamos entonces el ordenador y abrimos las configuraciones de la BIOS (presionamos las teclas «Supr.», «F1», «F2» o «F12» dependiendo de la BIOS que tengamos). Después, abrimos las opciones avanzadas de la propia BIOS. Cambiamos el campo del dispositivo de arranque a *HDD* (disco duro).



Eliminar un virus de command.com »

Windows

Si el software antivirus no es capaz de eliminar un virus que ha infectado al comando encargado de interpretar *command.com*, entonces tendremos que encargarnos de eliminarlo manualmente.
Pedimos a alguien que utilice la misma versión de Windows que nosotros que nos cree un disco de arranque. Copiamos los archivos *sys.com* y *fdisk.exe* de *c:\windows\conmand* al disco de arranque. Iniciamos nuestra máquina en el modo DOS con el disco de arranque.
Ejecutamos *sys c:* para crear una copia limpia de *command.com* en el disco C:\. Si no solucionamos el problema, creamos un nuevo disco de arranque master con *fdisk/mbr*. Lo último sería formatear el disco duro y reinstalar el sistema operativo.



Este mensaje es un *hoax*, no debemos eliminar el archivo *jdbgmgr.exe*.

Cuidado con *jdbgmgr.exe* »

Windows y *hoaxes*

¿Has recibido algún e-mail en el que te avisa de que un archivo llamado *jdbgmgr.exe* puede dañar tu sistema y te invita a eliminarlo? Esta notificación es falsa tratándose de un *hoax* muy peligroso. El archivo es parte de Windows y no debe eliminarse, ya que se requiere para cada una de las aplicaciones de Java. El icono del programa es incluso adjuntado en el mensaje de correo electrónico. Si nuestro antivirus nos avisa de que el archivo ha sido infectado, entonces puede haber caído presa de un virus. De este modo, seguimos las instrucciones de nuestro software antivirus.

Un correo será confidencial si el mensaje está encriptado

Si envías un *e-mail* a través de Internet, corres el riesgo de distribuirlo a todo el mundo. La solución pasa por la encriptación de mensajes.

Usa mensajes con texto sin formato »

Todos los clientes de correo

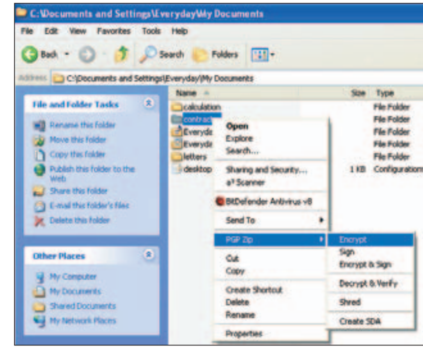
La encriptación trabaja mejor con aquellos mensajes que están escritos con un texto sin formato. Los *e-mails* que emplean el lenguaje HTML pueden llevar consigo problemas de verificación de la firma digital. En Outlook Express, puedes desactivar la opción de correo HTML, abriendo el menú *Herramientas* y haciendo clic en *Opciones*. Haz clic en la pestaña *Enviar* y selecciona el campo *Texto sin formato*, debajo de *Configuración de formato de envío de correo*. Deberías, además, desactivar la opción *Responder a los mensajes en el formato en que fueron enviado.*

Asegúrate de que todos los correos se envían como texto sin formato.

Encriptando archivos y carpetas »

PGP Desktop

Si cuentas con el programa PGP Desktop, puedes emplearlo para encriptar los archivos y las carpetas almacenadas en el disco duro del PC. Durante su configuración, el programa se añade a los menús de contexto de Windows Explorer. Para encriptar un archivo o una carpeta, haz clic sobre ellos con el botón derecho de tu ratón dentro de Explorer. Pulsa sobre *PGP Zip* y, a continuación, en *Encrypt*. Selecciona tu clave, a partir del listado que posees, y haz clic en *OK*. Cuando encriptes una carpeta, todos los archivos y carpetas que almacene serán encriptados también. Además, cualquier archivo puede copiarse o moverse a la carpeta encriptada más tarde de manera automática. PGP Desktop descifra archivos codificados tan pronto como los abras con una aplicación o a través de Explorer. Por razones de seguridad, puedes determinar que PGP te solicite tu contraseña cada vez que intentes descifrar un archivo o una carpeta (ver la siguiente pista).

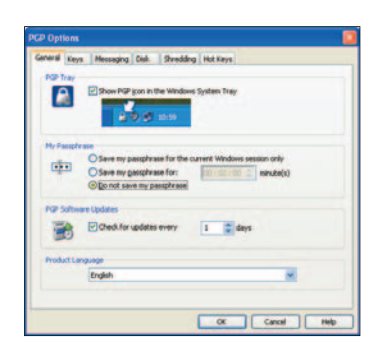


PGP Desktop permite encriptar archivos y carpetas.

Más seguridad, menor conveniencia »

PGP Desktop

PGP normalmente nos recordará nuestra contraseña una vez que la hemos registrado en el programa. Esto significa que no tendremos que introducirla cada vez que encriptemos o desencriptemos mensajes o archivos. El inconveniente es que cualquier persona que pueda tener un acceso físico a nuestro ordenador, mientras permanecemos alejados de nuestro escritorio, podrá descifrar los mensajes almacenados en el disco duro. Para prevenir esto tienes dos alternativas: o proteger tu máquina con un salvapantallas que se desbloquea con una contraseña o detener a PGP solicitándonos la contraseña. Localizaremos *Options*. Ahora, abre la pestaña *General* y acepta una de estas dos opciones: *Save my passphrase for 5 minutes* o *Do not save my passphrase* (es la alternativa más segura).

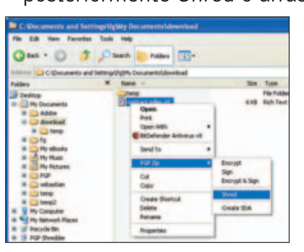


Si a menudo permaneces fuera de la oficina, deshabilita la opción que permite a PGP guardar nuestra contraseña. Así, ningún intruso manipulará tus correos y archivos encriptados.

Elimina documentos delicados »

PGP Desktop

Dentro de PGP Desktop hay un archivo de seguridad que borra definitivamente algunos archivos para que no puedan ser recuperados. Después de su instalación, verás el icono *PGP Shredder* en tu *Escritorio*. Para borrar un archivo, arrástralo hasta dicho icono. De forma alternativa, desde el Explorador de Windows, marca ese archivo con el botón derecho del ratón y selecciona *PGP Zip* y posteriormente *Shred* o arrastra el archivo al icono *PGP Shredder* en el Explorador (debajo de la *Papelera de reciclaje*).



Para prevenir que un archivo suprimido sea restaurado, tendrás que eliminarlo con la ayuda de PGP Shredder.



GPA (*Gnu Privacy Assistant*) es una interfaz gráfica de código abierto.

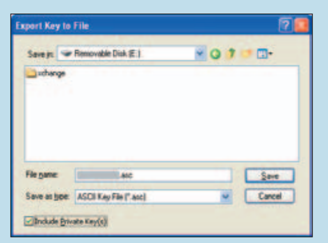
Alternativa gratuita a PGP »

GnuPG

Si prefieres un software de Código Abierto y no quieres pagar por PGP Desktop o si ejecutas Linux, podrías probar las bondades de GnuPG. Compatible con PGP Desktop, está preparado para descifrar correos y archivos encriptados utilizando PGP y viceversa. De todas maneras, debes saber que GnuPG está disponible únicamente como una herramienta de línea de comandos. Para hacer de esta herramienta algo más amigable, puedes emplear una interfaz gráfica como GPA (Gnu Privacy Assistant) o WinPT. Para obtener el programa GuPG y uno de sus entornos gráficos, abre la página **www.gnupg.org** en tu navegador web y descárgate las herramientas.

Asegura tus claves »

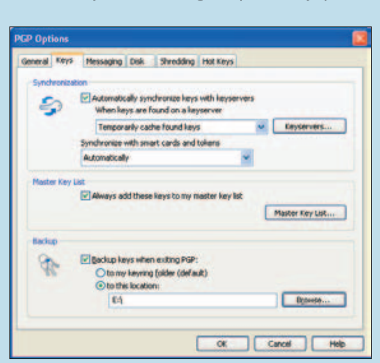
PGP Desktop



Crea una copia de seguridad de tu clave privada en un disquete o en una llave USB.

Sin tu clave privada, no serás capaz de descifrar los mensajes y archivos que recibas. Por este motivo, podrías crear una copia en un disco externo, como un disquete o una llave USB. Abre PGP Desktop, selecciona tu clave y nómbrala a través de la ruta *File/Export/Key*. Selecciona el lugar donde quieres almacenar tu clave y asegúrate de que activas la opción *Private Key(s)* antes de hacer clic en *Save*. Eso sí: recuerda que no tienes que dar tu clave a ninguna persona.

Sigue la ruta *File/Export/Keyring*. Para tener tus claves copiadas automáticamente cuando salgas de PGP, abre la caja de diálogo *Options* y pulsa la pestaña *Keys*. Activa *Backup keys* cuando salgas de esta aplicación, además de *To this location* y selecciona un disquete o dispositivo USB.

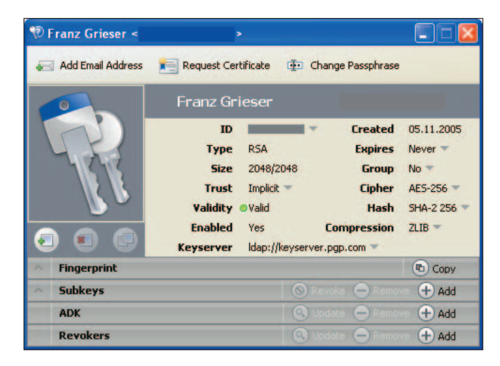


Puedes tener tus claves guardadas automáticamente cuando salgas de PGP.

Cambiar las configuraciones de tu clave »

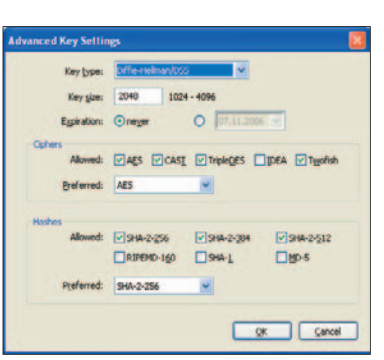
PGP

PGP usa tres algoritmos diferentes. RSA y Diffie Hellman se emplean para encriptar las claves dentro de un correo o un archivo. Aunque ambos algoritmos se consideran seguros, suele preferirse RSA por razones de compatibilidad y porque ya se utilizaba en las primeras versiones de PGP. Mientras, el algoritmo por defecto para encriptar información es AES (la única alternativa viable aquí es Twofish, que es tan segura como AES. TripleDES no tiene la consideración de segura). Los otros dos algoritmos (CAST e IDEA), no deberían utilizarse. Para comprobar si el correo o archivo encriptado ha sido forzado, PGP emplea un código encriptado que se denomina *hash*. Aquí SHA-2 con claves de 256 bits resultará adecuado



Para cambiar las configuraciones *Cipher* o *Hash* de una clave existente, abre la caja de diálogo *Key Properties* de PGP Desktop.

Si uno de tus compañeros de comunicación no puede descifrar los correos electrónicos que le envías quizás tengas que cambiar las configuraciones de tu clave. Para una clave que ya exista, necesitarás cambiar el *cipher* (cifra, como AES, Twofish)) y el *hash* (los ejemplos incluyen SHA-2). Para modificar estas dos configuraciones, haz clic con el botón derecho del ratón en la clave en cuestión, dentro de PGP, y selecciona otro *cipher* o *hash*. Si deseas modificar el tipo de clave pública (RSA o Diffie-Hellman), porque alguien te intercambia correos encriptados utilizando Diffie-Hellman, en vez del tipo RSA que hay por defecto, deberás crear un nuevo par de claves. Dentro de PGP Desktop sigue la ruta *File/New PGP* y sigue las instrucciones que el Asistente te indicará en pantalla. En la página *On the Name and Email Assignment* introduce tu nombre y dirección de correo. A continuación, pulsa el botón *Advanced*. Selecciona el tipo de clave que escojas (en nuestro caso ha sido *Diffie-Hellman/DSS)* y ajusta el resto de las configuraciones de acuerdo a tus necesidades. Procede tal y como se describe el paso a paso y no olvides crear una copia de seguridad de tus claves.



Si necesitas un tipo de clave distinta (de tipo RSA o Diffie-Hellman), tendrás que crear un par de claves nuevas.

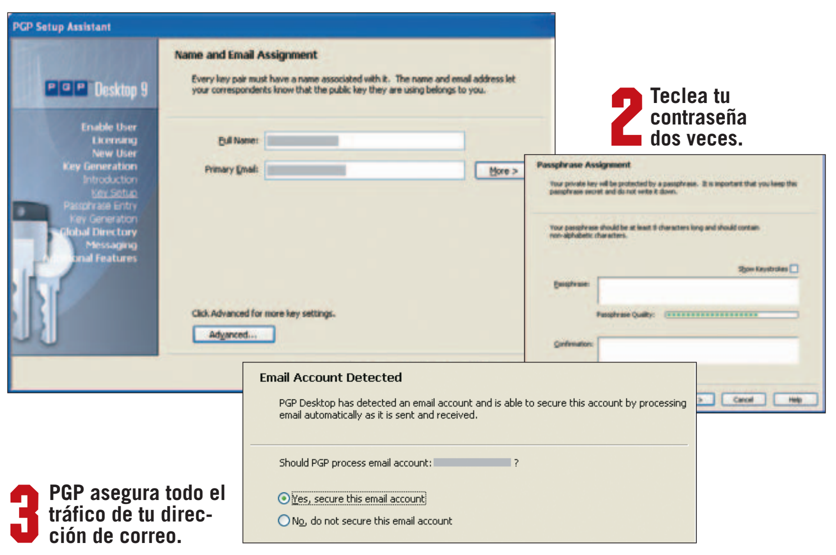
Cómo encriptar el correo electrónico con PGP

Enviar mensajes y archivos confidenciales a través del correo electrónico es como escribir una tarjeta postal, meterla en el buzón y confiar en que el cartero no sea curioso. Si realmente deseas que la información que manejas sea confidencial, deberás recurrir a la encriptación.

La mejor herramientas que existe, en estos instantes, para tareas de encriptación es PGP Desktop (www.pgp.com). Aunque ésta ha sido gratuita durante años siempre y cuando hiciésemos un uso personal de la misma, sus desarrolladores han optado por ofrecer únicamente una versión comercial (eso si, podemos probar durante 30 días el programa gratis). ¿Desearías intercambiar correos encriptados sobre otras plataformas informáticas como Windows, Mac o Linux? No hay mejor elección. Además, PGP Desktop no sólo protege correos y archivos adjuntos, pues también lo hace sobre comunicaciones de mensajería (a través de AOL), encriptando, además, archivos y carpetas del disco duro. Por este motivo, hemos escogido PGP como ejemplo para el siguiente práctico.

En el caso de que no quieras gastarte 105 euros, es el precio que vale la herramienta, existe una edición gratuita llamada GnuPG (ver la sección de pistas), disponible para la mayoría de las plataformas informáticas.

Desafortunadamente, se trata de una herramienta de líneas de comando, un tanto anticuada, aunque presenta algunas pantallas gráficas para facilitar su utilización. Cuando emplees PGP u otra herramienta de encriptación gratuita, es muy importante que entiendas el concepto de uso público y privado de las claves (ver recuadro de la página 81).



1 Introduce tu nombre y tu dirección de correo.

2 Teclea tu contraseña dos veces.

3 PGP asegura todo el tráfico de tu dirección de correo.

1 Configurar PGP

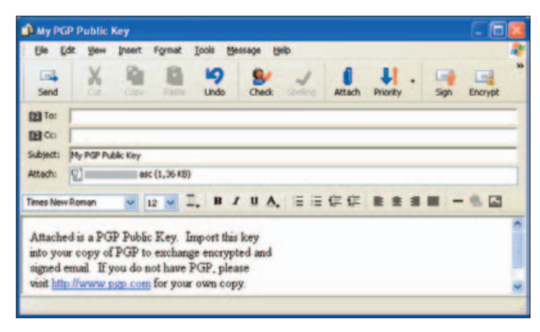
Cierra tu cliente de correo e instala PGP Desktop en tu sistema siguiendo las instrucciones del Asistente que aparecerá en pantalla. Cuando lo hayas hecho, se te preguntará si has utilizado el programa en alguna otra ocasión. Nosotros especificaremos que es la primera vez que lo vamos a usar. Tras esto, haremos clic en los botones *Next* y *Next*. Introduce tu nombre y tu dirección de correo electrónico. Normalmente, puedes mantener las configuraciones de la clave por defecto (más información sobre la configuración de las claves y algoritmos en la sección de pistas). No obstante, si quieres modificar una configuración, pulsa el botón *Advanced*. Para proceder, pulsa en *Next*.

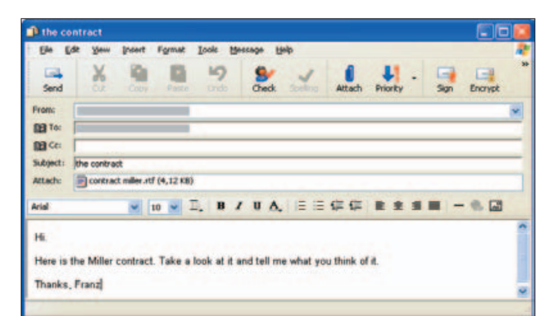
2 Introduce una contraseña

Tu clave privada es protegida por una contraseña. Escoge una cuidadosamente y mantenla en secreto, pues ten en cuenta que si alguien se hace con tu equipo y tu clave privada, sólo necesitará ésta para descifrar los correos que te envían, suplantando, así, tu identidad. Desactiva la opción *Show Keystrokes*. Ahora escribe la contraseña dos veces y pulsa *Next*. PGP generará tu par de claves. Marca *Next* dos veces más para proceder, enviando la pública al servidor Global Directory. Vuelve a hacer un clic en *Next* otras dos veces para que PGP pueda, automáticamente, detectar tus cuentas de correo. Lee la política establecida para el correo electrónico y acéptala. Haz clic en *Finish*.

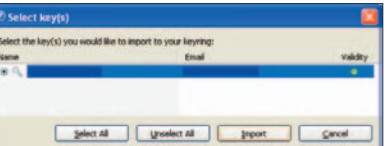
3 Prepara tu cliente de correo

Es el momento de que aparezca en pantalla tu cliente de correo. Cuando se trate de un software conocido por PGP (como por ejemplo Outlook o Thunderbird), visualizarás un mensaje que te ofrecerá proteger la cuenta para la que has generado ese par de claves.
Acéptalo y haz clic en *Next*. Para utilizar el par de claves que acabas de crear, selecciona la opción *PGP Desktop Key* y pulsa *Next* (de otra manera, tendrás una nueva clave generada o importada una ya existente pero que todavía no está incluida en tu listado personal). Selecciona tu clave de la lista que aparecerá y sigue la ruta *Next/Finish*.





4 Envía tu clave pública a través del correo a amigos y familiares



5 Importa la clave pública que has recibido por correo.

6 Para encriptar y firmar un correo sólo tienes que introducir el nombre de tu destinatario, cuya llave pública conocerás de antemano.

4 Transmite tu llave pública

Tus familiares y amigos necesitan tu llave pública para enviarte correos encriptados. Para dársela, prueba a mandarles un correo. Nuestro punto de partida será PGP Desktop Ahora, marcamos *Open PGP Desktop* y seleccionamos nuestra clave. Hacemos clic sobre *E-mail this key link*, en la parte izquierda de la pantalla. PGP abrirá tu correo para que redactes tu texto y añadas tu clave. Incluye las direcciones de los destinatarios y envíales ésta.

5 Importa otras llaves

Tienes que preguntar a la gente a la que quieres hacer llegar un correo encriptado que te hagan llegar sus respectivas llaves públicas. Cuando recibes un *e-mail* que contenga una clave pública, abre el adjunto (el archivo en cuestión contendrá la clave). Ahora, PGP te preguntará si deseas importar dicha clave. Pulsa sobre el botón *Import* para que la clave que hayas recibido pase a formar parte del listado de PGP Desktop.

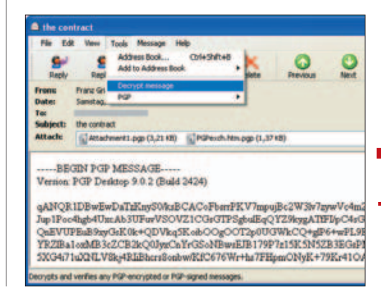


6 Encripta y firma correos

Redacta un nuevo correo electrónico. En el campo *Para*, añade a todos aquellos destinatarios cuya clave pública tengas. Tan pronto como marques el botón *Enviar*, PGP encriptará tu correo y los archivos que hayas podido adjuntar empleando la clave pública de tus destinatarios. Es posible que desees firmar el correo y los elementos adjuntos con tu clave privada. Piensa que de esta manera el receptor de tu correo se asegurará que realmente el correo que ha recibido es tuyo, siendo la única persona que puede leer su contenido (piensa, además, que es el único que posee esta clave privada). Verás que tu cliente de correo (en nuestro caso Outlook Express) cuenta con los botones *Firmar* y *Cifrar*. No hagas clic sobre ellos. ¿El motivo? Se emplean para encriptar y firmar mensajes utilizando un certificado digital y no para utilizar las claves de PGP.

7 Desencriptar y verificar correos

Cuando recibes un mensaje encriptado y lo abres, sólo verás una jerga sin ningún tipo de significado. Abre el menú *Herramientas* y selecciona *Cifrar*. PGP, ahora, verificará esta firma y descifrará el cuerpo del mensaje (los adjuntos aún no). Cuando PGP determina que la firma es correcta, añadirá una línea que dirá *Status: Good Signature* para «entender» el correo. Para un archivo adjunto, haz un doble clic en el fichero *Attachment.pgp* y ábrelo. PGP Desktop será el encargado de desencriptar el archivo dentro de la ventana. Haz un doble clic en el archivo y selecciona la opción *Extrat to save the decrypted file on your hard disk.*



7 PGP descifra los correos encriptados.

Par de claves

La encriptación requiere una clave, que es necesaria para poder manipular el texto comprimido en un correo o en un archivo. Un algoritmo de encriptación utiliza la clave para convertir tu mensaje o archivo en una secuencia de caracteres que no tienen sentido alguno. El destinatario emplea la misma clave para descifrar el mensaje y convertirlo en un texto plano otra vez.

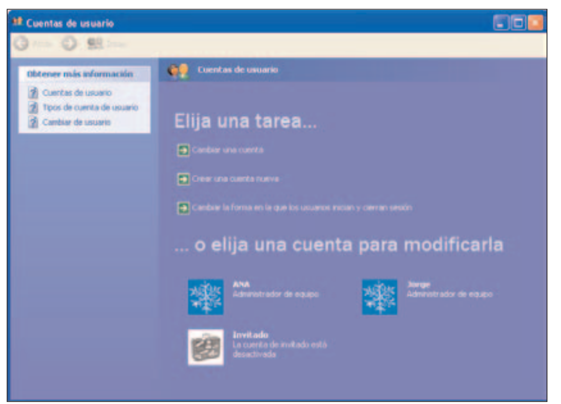
Existen dos tipos de encriptación. En la simétrica, la misma clave se emplea para encriptar y descifrar. El problema aquí es que tienes que dar a los destinatarios de los mensajes tu clave. Si intercambias correos únicamente con una o dos personas, intercambiarla y mantenerla en secreto es algo factible. Si, de todas maneras, intercambias mensajes confidenciales con un montón de personas, algunas de las cuales no conoces personalmente, no resultará muy práctico que empleen tu clave.

El otro tipo de encriptación se denomina asimétrica (o llave pública de encriptación). Aquí tienes dos tipos de llaves: una pública para encriptar y otra privada para descifrar. Damos la llave pública pública a alguien que quiere enviar un correo encriptado. Mientras, la privada se requiere para descifrar los correos que nos envían (ellos sólo podrán descifrarlos utilizando nuestra llave privada). Resulta fundamental mantener esta clave en secreto.

El intercambio de claves no es un problema con la encriptación asimétrica. Sólo tienes que transmitir tu clave enviándola a tus amigos y familiares a través del correo y poniéndola en un servidor público de claves (tarea que PGP puede hacer por ti, si así lo deseas). Mientras, colecciona claves públicas de amigos y familiares y grábalas en el listado que PGP te facilita para que puedas enviarles correos encriptados.

Prohibido el paso a la red

Desde siempre, Windows ha sido el sistema más hackeado, dada su gran popularidad y ciertas debilidades. Sin embargo, no es en absoluto un mal gestor de los PCs; tan sólo será necesario reforzar en lo posible la seguridad que ofrece.



Por razones de seguridad ejecutamos Windows en una cuenta limitada.

Una cuenta limitada para el día a día »

Windows

Una de las configuraciones de seguridad más importantes son los privilegios de usuario. Es decir, conceder permiso a aquellos usuarios que necesiten información procedente de nuestro ordenador para completar su trabajo. Si los usuarios tuvieran más derechos de lo debido, podrían hacer mal uso de los datos contenidos en nuestra máquina. Y si ejecutamos nuestro sistema utilizando los máximos privilegios posibles, el modo administrador de Windows, cualquier usuario podría disponer de todos los permisos y causar algún tipo de daño.
Lo más inteligente va a ser ejecutar un ordenador bajo Windows a través de una cuenta con permisos limitados. Una vez instalado, Windows XP por defecto se ejecuta en el modo administrador, por lo que debemos configurar una cuenta limitada que será la que utilicemos habitualmente. Este tipo de cuenta tiene sus propios inconvenientes que intentaremos salvar siguiendo los siguientes pasos.

Sólo en modo administrador »

Lista de Windows

Microsoft cuenta con una lista de unas 100 aplicaciones que sólo funcionan cuando se lanzan a través de una cuenta de administrador. Entre ellas encontramos, como dato curioso, algunas versiones de Microsoft Money y Flight Simulator 2004. Vamos a **http//support.microsoft.com** en busca de ayuda en el caso de que alguna aplicación se comporte de una forma extraña. De todas formas, en el siguiente paso incluimos un truco que permite ejecutar cualquiera de estos programas en una cuenta limitada.



En *http//support.microsoft.com* encontraremos ayuda si alguna de nuestras aplicaciones se comporta de forma extraña.

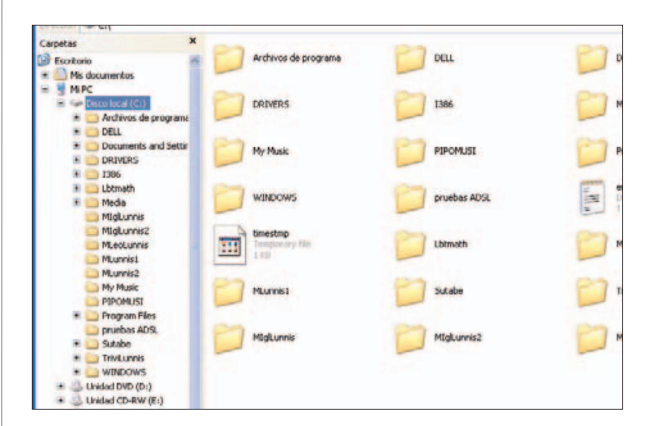
Instalar el software a través de una cuenta limitada »

Windows

Si no tenemos los privilegios de un administrador, entonces no podemos instalar ningún tipo de software en nuestra máquina. En ese caso lo más habitual es cambiar a una cuenta de administrador, instalar el software, volver a la cuenta limitada e iniciar el programa.

Sin embargo, mucho más sencillo es hacer uso de la opción *Ejecutar como* de la que está provisto Windows XP y 2000. Así hacemos clic con el botón derecho del ratón sobre cualquier archivo *.exe*, seleccionamos *Ejecutar como* y especificamos las credenciales de administrador para instalar el programa. Sin embargo, esta opción no está disponible en archivos *.msi*, por lo que utilizamos *Ejecutar como* para abrir una ventana de comando (*cmd.exe*) con los credenciales de administrador y ejecutamos el archivo *.msi* para instalar la aplicación.

La instalación de algunas programas con privilegios de administrador, utilizando la opción *Ejecutar como* puede causar algunos problemas. Así no funcionan adecuadamente cuando las ejecutamos como usuario normal. Esto se debe a que la rutina de instalación crea configuraciones de usuario únicamente para el perfil de administrador.

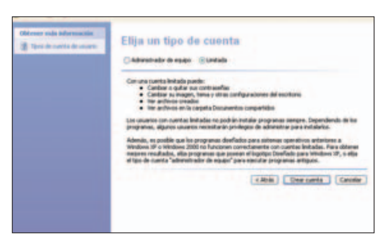


Internet Explorer puede utilizarse como una alternativa al Explorador de Windows.

Compartir con una cuenta limitada »

Explorer

Abrimos el Explorador de Windows (*explorer.exe*) y hacemos clic con el botón derecho del ratón sobre una carpeta, si estamos trabajando con una cuenta limitada no aparecerá la opción *Compartir*. Por su parte, la alternativa *Ejecutar como* no funciona con Windows Explorer. De este modo, utilizamos la opción *Ejecutar como* para iniciar Internet Explorer (*iexplore.exe*) en vez de *explorer.exe*. Un vez abierto Internet Explorer, tecleamos *C:* en la barra de direcciones y pinchamos en el botón *Carpetas* de la barra de herramientas por lo que nos mostrará una interfaz similar a la del Explorador de Windows. Navegamos hasta la carpeta que queremos compartir, hacemos clic con el botón derecho del ratón y seleccionamos *Compartir y seguridad*.



Créate una cuenta limitada para las tareas cotidianas.

Una cuenta con derechos limitados »

Windows

Para crear una nueva cuenta, nos registrarnos con permisos de administrador. Seleccionamos *Inicio/Panel de control/Cuentas de usuario*. Pinchamos en *Crear una nueva cuenta*, introducimos el nombre y pinchamos en el botón *Siguiente*. Elegimos el tipo de cuenta y pulsamos en el botón *Crear una cuenta nueva*. Si queremos proteger esta cuenta, pinchamos en el nombre de cuenta en la lista y seleccionamos *Crear una contraseña*. Introducimos la contraseña dos veces.

Problemas de una cuenta limitada »

Windows

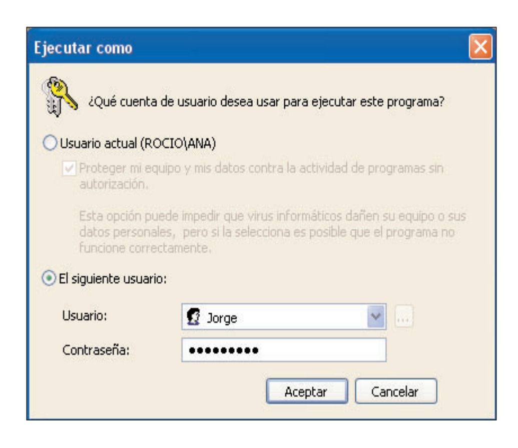
Cuando ejecutamos el ordenador bajo una cuenta limitada, no todo funciona en Windows como debiera. De este modo pueden surgir problemas como:

- Así por ejemplo al instalar cualquier tipo de software, suele fallar mostrando algún tipo de error.
- También a la hora de ajustar la fecha y la hora en el Panel de control, aparece una caja de diálogo que nos dice que no tenemos suficientes privilegios para ello.
- Lo mismo ocurre cuando intentamos configurar las *Opciones de energía* en el Panel de control. Tan pronto como queremos aplicar los cambios en esta carpeta aparece una ventana que nos deniega esta acción.
- Es imposible compartir una carpeta en nuestra máquina para que otro usuario pueda acceder a ella, ya que no aparece la opción *Compartir* en el menú de *Propiedades*.

Incluimos en las siguientes páginas la solución para los tres últimos inconvenientes.

En una cuenta limitada no es posible cambiar la fecha y hora o las opciones de energía.





Es posible ejecutar un programa una vez a través de una cuenta de administrador.

Ejecutar en modo administrador »

Windows

Hacemos clic con el botón derecho del ratón sobre el nombre del programa y seleccionamos *Ejecutar como*. Marcamos la opción *El siguiente usuario*, seleccionamos el nombre de usuario, introducimos la contraseña y pinchamos en *Aceptar*.

Cambiar el perfil de usuario rápidamente »

Windows

Cuando utilizamos una cuenta con derechos de usuario restringidos, más pronto o más tarde necesitaremos la ayuda del administrador para ejecutar o instalar algún programa. Cambiar los perfiles a través de *Inicio/Cerrar sesión/Cambiar de usuario* nos llevará algo de tiempo. Sin embargo, a través de la opción *Ejecutar como* será posible abrir una aplicación utilizando distintos perfiles. Vamos a *Inicio/Ejecutuar* e introducimos *runas/profile/user:Computer/Administrator cmd*. De este modo, obtendremos la contraseña del administrador. Una vez realizado esto ejecutamos Windows como administrador. Creamos un icono en el Escritorio que invoque a *Inicio/Ejectuar* y ejecutamos la instrucción o bien seleccionamos la instrucción de la lista de la caja de diálogo *Inicio/Ejecutar*.

Crear una cuenta de administrador falsa »

Windows

Protegemos nuestro equipo configurando una cuenta que simule ser el administrador. Creamos una cuenta que se llame *admin.* o *administrador* pero le damos sólo permisos limitados. Configuramos una contraseña difícil para esa cuenta.

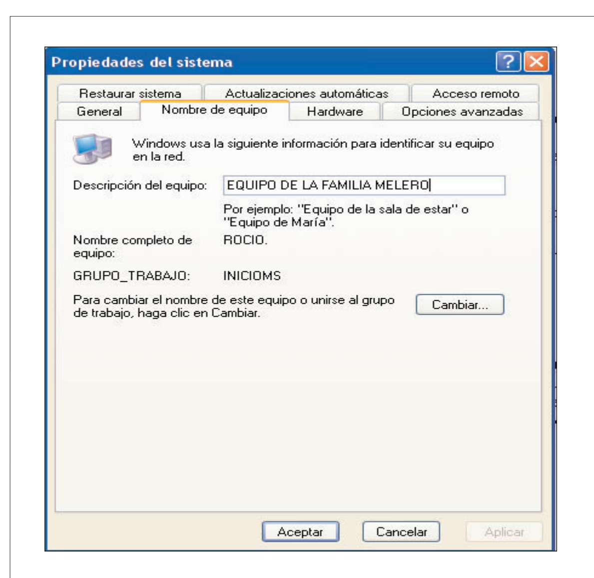
Cualquier usuario puede creer que esta cuenta es la que cuenta con privilegios de administrador.

Derechos de administrador »

Windows

Si tenemos una aplicación que requiere derechos de administrador para ejecutarse adecuadamente, podemos conceder acceso como administrador a ese programa siguiendo los siguientes pasos. Hacemos clic con el botón derecho del ratón sobre el nombre del programa y seleccionamos *Propiedades*. Pinchamos en el botón *Propiedades avanzadas*, seleccionamos *Ejecutar con credenciales diferentes* y luego hacemos clic en *Aceptar*. Lanzamos la aplicación y tan pronto como se abra, introducimos el ID de administrador y por último la contraseña.

Podemos conceder privilegios a aplicaciones para que se ejecuten a través de la cuenta de administrador.



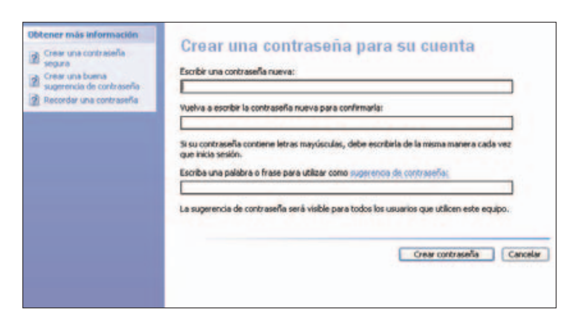
Solamente la cuenta de administrador puede cambiar el nombre del ordenador.

Comprobar el tipo de cuenta »

Windows

Contamos con dos métodos para verificar si somos o no el administrador:

- Hacemos clic con el botón derecho del ratón sobre *Inicio*. Si nos muestra la opción *Explorar todos los usuarios*, estamos trabajando como administrador.
- Hacemos clic con el botón derecho del ratón en el icono *Mi PC*, seleccionamos *Propiedades* y resaltamos la pestaña *Nombre de equipo*. Si podemos pinchar en el botón *Cambiar*, quiere decir que tenemos permisos de administrador.



Protegemos nuestras cuentas con contraseñas.

Configurar una contraseña »

Windows

Incluso si decidimos no crear ni utilizar una cuenta limitada, debemos proteger nuestra cuenta de administrador a través de una contraseña. Abrimos *Inicio/Panel de control/Cuentas de usuario*. Seleccionamos la cuenta de administrador y pinchamos en el enlace *Crear una contraseña*. Introducimos dos veces la contraseña y una pista que nos ayuda a recordarla. Pinchamos en *Crear contraseña*.

Utilizar Windows Update en una cuenta limitada »

Windows

La actual versión de Windows Update y Microsoft Update no se ejecutan con la opción *Ejecutar como*. Utilizamos las actualizaciones automáticas, abrimos la cuenta de administrador, ejecutamos Windows Update y volvemos otra vez a la cuenta limitada.

Jugar en una cuenta limitada »

SafeDisc

Cuando ejecutamos una cuenta restringida, algunos juegos no se iniciarán correctamente. Incluso aunque tengamos el disco en la unidad, el juego nos pedirá que lo insertemos. La solución está en descargarnos la herramienta SafeDisc proporcionada por Microsoft. Esta no alterará ningún componente de nuestro sistema, sólo cambiará el estado de inicio del componente necesario para iniciar el juego. Podemos descargarnos SafeDisc de **http://go.microsoft.com/?linkid=3124926**. Instalamos la herramienta desde la cuenta con privilegios administrativos.

Quick Info	
File Name:	safedisc.exe
Version:	1.0
Date Published:	4/28/2005

Microsoft cuenta con una herramienta que nos permite jugar desde una cuenta limitada.

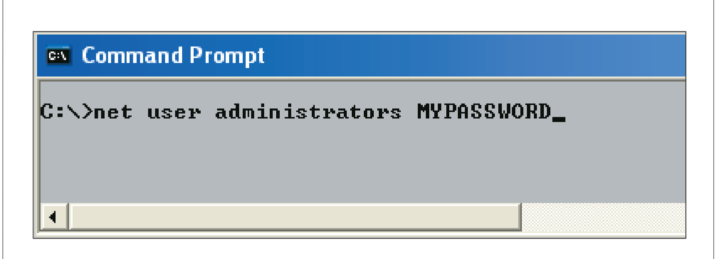
Fecha, hora y opciones de energía »

Panel de control

El árbol de carpetas de Internet Explorer visualiza el icono Panel de control. Seleccionamos este icono y en el panel de mano derecha aparecerán las distintas opciones. Utilizamos *Fecha y hora* para cambiar la hora en nuestro sistema. Como Internet Explorer trabaja bajo el modo administrador, todos los programas a los que accedemos a través de él cuentan con credenciales de administrador. Lo mismo ocurre con las *Opciones de energía*, las *Conexiones de red* o el *Sistema*.



Internet Explorer puede utilizarse como un sustituto del Explorador de Windows.



Use the Net User Administrator's command to quickly change an account's password.

Configurar una contraseña de administrador rápidamente »

Windows

Un modo rápido de introducir una contraseña de administrador es abrir la ventana *Ejecutar* e introducir la línea:

net user administrador MICONTRASEÑA

En lugar de MICONTRASEÑA introducimos la nueva contraseña. Verificamos que hemos tecleado la contraseña correctamente antes de pulsar en la tecla *Intro.*



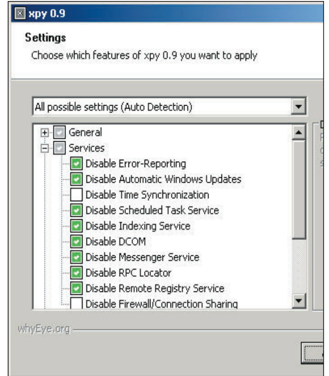
Preguntas y respuestas

Averigua los programas que se autoejecutan y elimínalos; no tomes como verdaderos los correos cuyo remitente sea «Microsoft» y actualiza el antivirus de tu ordenador.

? Hay varios programas y servicios que aparecen automáticamente al iniciar Windows, pero sólo puedo localizar unos cuantos en el menú *Inicio*¿Cómo puedo saber qué software se inicia de manera automática y cómo detener los programas que no quiero ejecutar?

! Existe un número de localizaciones dentro de Windows en las que se autoejecutan aplicaciones que pueden ocultarse, en particular, dentro del Registro. Afortunadamente, existe una herramienta gratuita que conoce todas estas localizaciones y enumera los programas que automáticamente aparecen al inicio. Nos estamos refiriendo a Autoruns (**www.sysinternals.com/Utilities/Autoruns/html**). Descarga esta herramienta y cópiatela. Ahora, crea un enlace al menú *Inicio* o a tu *Escritorio*. Ya con Autoruns, lo que haremos será abrir la pestaña *Everything*. Navega a través de la lista que te aparecerá y deshabilita todos los programas que no quieres que se inicien de manera automática. Si deseas aprender algo más sobre una entrada de la lista en particular, selecciona el comando *Properties* del menú de contexto o navega a través de Google.
La pestaña *Services* muestra los servicios (de Microsoft y otras compañías) que se están ejecutando y explica para qué sirven. Otra herramienta útil es Xpy (**http://sourceforge.net/projects/xpy**), que permite inhabilitar las características referidas a la comunicación de Windows que pueden ser «explotadas» por programas *spyware* y software de tipo malicioso, como Microsoft Messenger, Media Player y servicios remotos como RPC Locator.

Autoruns muestra los programas y servicios que automáticamente aparecen al iniciar Windows.



Xpy permite deshabilitar las funciones de comunicación de Windows como Windows Messenger.

? He recibido un mensaje que contiene una actualización de seguridad procedente de Microsoft. ¿Cómo puedo saber que dicho correo es auténtico?

! Las compañías serias de software no envían actualizaciones de seguridad a través del correo electrónico (piensa en el enorme coste que acarrearía la cantidad de información que necesitan transferirse). En el caso de que notifiquen a sus usuarios las actualizaciones correspondientes a través de esta vía, incluirán un enlace a su web o FTP donde podrás conseguir la correspondiente actualización. Algunas compañías, entre ellas Microsoft, también firman sus notificaciones añadiendo una firma PGP.
Si llega a tu correo un mensaje de estas características, no pulses sobre su enlace. Más bien, copia el *link* al campo de dirección de tu navegador y comprueba, con mucho cuidado antes de abrir la página web correspondiente, si ésta es realmente una dirección «Microsoft.com» (y no una dirección con una ortografía errónea del tipo «mirosoft.com» que alguien le ha enviado para atraerle a su espacio).
El mensaje que recibiste probablemente contenga el gusano Gibe.B o uno de sus numerosos sucesores. Esta familia de código malicioso hizo su primera aparición en marzo de 2002, alcanzando «su momento cumbre» en septiembre de 2003. El gusano toma el disfraz de una alarma de seguridad proveniente de Microsoft, reclamando tu atención para tapar alguno de los huecos de seguridad existentes y, de paso, tratando de engañar a sus destinatarios para que ejecuten el archivo adjunto ejecutable. Si un usuario cae en la trampa, el gusano se instalará (en algunos casos también lo hará un troyano que establecerá una puerta trasera en el sistema) y se enviará a sí mismo a todas las direcciones de correo que encuentre. Si empleas un escaneador de virus y éste no te ha notificado la existencia de gusanos, asegúrate que tienes instaladas sus últimas actualizaciones.

? Tengo un determinado número de herramientas que de forma automática aparecen cuando inicio Windows. En algunas ocasiones no deseo que esto suceda por que no las voy a necesitar.

! La solución es un simple atajo de teclado. Enciende o reinicia Windows. Tan pronto como la ventana de bienvenida aparezca, presiona la tecla «Mayúsculas» hasta que el sistema operativo acabe de cargarse en su totalidad.

CONTRAESPÍAS



Por si no tuviésemos bastante con los virus, los hackers y los troyanos, existen también espías capaces de infiltrarse en nuestros ordenadores sin que lleguemos a darnos cuenta. ¡Es hora de acabar con ellos!

George Orwell tenía razón... Alguien te vigila

Parece como si en la actualidad unos ojos electrónicos fueran siguiéndote por todos lados y rastreando cada paso que das. Sin embargo, puedes hacer mucho para mantener tu información digital a salvo de espías

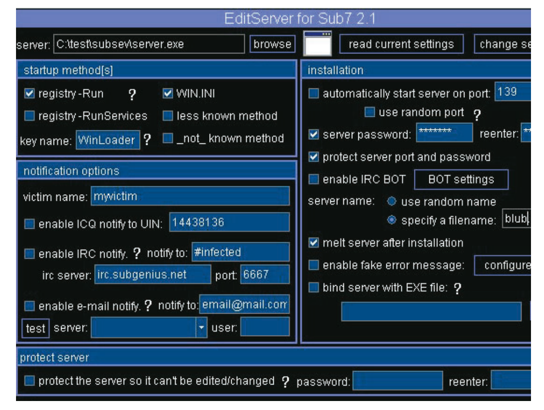
La mayoría de la gente ni siquiera se da cuenta de que estamos continuamente expuestos a ser espiados cuando trabajamos con ordenadores. Piensa en tu oficina: muchos de los programas que utilizamos son en general benignos, pero pueden ser utilizados para vigilarnos. Las soluciones de gestión de red ofrecen funciones de registro que pueden ser utilizadas para rastrear las actividades de los empleados. Aplicaciones de seguridad de contenidos como Mimesweeper (**www.mimesweeper.com**) filtran tu bandeja de correo y eliminan correos indeseados. Pero pueden escanear también el correo de salida y la red local, utilizando términos de búsqueda adaptados y detectando archivos ilícitos. El software de control remoto confiere todos los derechos sobre los PCs locales a los administradores remotos (normalmente, tienen más opciones de configuración que el usuario local). Pueden acceder a tu ordenador en cualquier momento, incluso, si quieren, sin que tú lo sepas. Teóricamente, los empleados deben estar al corriente del uso de estos programas, ¿pero ocurre siempre así?

LOS ESPÍAS ESTÁN ENTRE NOSOTROS Las herramientas como Orvell (**www.orvell.com/eng**) funcionan localmente en los PCs usuarios. Registran sistemáticamente las entradas de los usuarios como claves, llamadas y visitas a la web, sin dejar constancia de que están funcionando. Orvell no puede verse en el gestor de tareas, no ralentiza el PC, no deja rastro en el registro de Windows y sus archivos de registro no pueden ser leídos por cualquiera. Si piensas en ello, estos programas ofrecen funciones que suelen encontrarse en los perniciosos troyanos (¡pero al contrario que éstos, puedes comprarlos legalmente en la tienda!)

Las herramientas que acabamos de mencionar suelen estar prohibidas en las redes empresariales, al menos para funcionar de forma invisible. ¿Pero es eso cierto? Aun así, los troyanos son mucho peores. Pueden afectar a cualquiera que se meta en Internet. Por ejemplo, pueden camuflarse como un juego gratuito; al instalarlos como un juego, se introducen en tu ordenador bajo la forma de un programa de servidor. Continuará enviando información a un atacante externo y actuará como una puerta de entrada para

cuando el hacker quiera controlar tu sistema. Tu teclado registrará, por ejemplo, el número de tu cuenta en cuanto lo escribas, enviando la información inmediatamente al atacante.

Un software sencillo y peligroso es el capturador de posiciones del teclado (*keylogger*), popular entre las fuerzas de seguridad del estado como el FBI, donde se utiliza para capturar las pulsaciones y pasar frases de sospechosos. Lo más preocupante (aparte de las implicaciones contra los derechos civiles) es que los hackers pueden utilizar la herramienta contra cualquiera de nosotros. Suelen formar parte de un programa troyano, la herramienta clásica del hacker. Sin embargo,



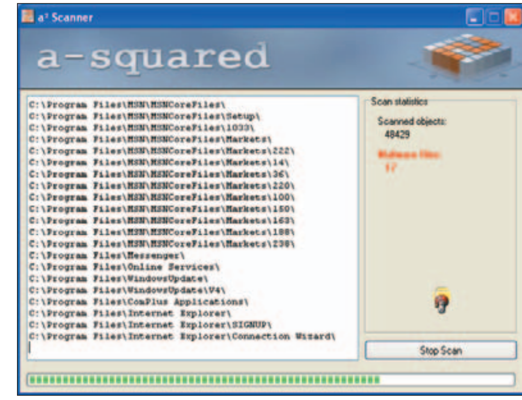
Abre puertas: un atacante puede configurar parte de un servidor Sub7 de tal manera que sea difícil detectarle.

pueden descargarla como utilidades independientes; por ejemplo, Key Interceptor o 2Spy. Los registradores de teclas anotan todas las teclas que presionas. No utilizan ninguna interfaz gráfica y operan en el entorno de la línea de comandos, por lo que consumen pocos recursos y son difíciles de localizar. Los hackers los utilizan para encontrar contraseñas, números de cuentas o datos de tarjetas de crédito.

EL MERCADO DE LOS HACKERS Y LOS VIRUS no es el único que puede suponer una amenaza para nosotros. Están también los insufribles vendedores. Sus métodos incluyen las *cookies* y los contenidos web manipulados que utilizan para enviar y almacenar permanentemente la información de los usuarios privados en un servidor central. Hablamos de los gusanos web, unas pequeñas imágenes GIF que activan órdenes CGI y envían información al servidor de origen. La información transmitida puede contener tu dirección IP, tu lenguaje de configuración, tu sistema operativo y el navegador que utilizas. Incluso tu cuenta de correo electrónico puede ser enviada. De esta forma, estos espías de información pueden crear un verdadero perfil de sus víctimas.

SI LA PÁGINA DE INICIO DE TU NAVEGADOR cambia de repente o tus peticiones de búsqueda te conducen siempre a otras páginas web, puedes estar seguro de que has sido víctima de un secuestro. Normalmente, esto se debe a JavaScript o ActiveX Control. Las herramientas especializadas como PestPatrol te ayudarán a detectar y eliminar a esos parásitos de los sistemas privados. Y además te protegerán de futuros ataques. Echa un vistazo a la utilidad gratuita SpywareBlaster, capaz de detener la instalación de los controles ActiveX malignos.

Si estás teniendo problemas de espionaje comercial no te preocupes, si inviertes un poco de tiempo podrás solucionarlo sin necesidad de instalar herramientas de protección especializadas. Sin embargo, es mucho más fácil combatir el espionaje con escáneres en línea (lee la columna adjunta) y herramientas de



La herramienta gratuita a-squared es excelente para proteger nuestro sistema del espionaje y los gusanos.

contraespionaje. Existen numerosos programas de este tipo y muchos de ellos son gratuitos, como Spybot Search y Destroy (**www.safer-networking.org**). Esta herramienta es muy sencilla y busca en tu registro las entradas más sospechosas. El software es excelente para rastrear malware, y te permite deshacerte de los programas indeseados con un solo clic.

Otra buena herramienta es a-squared Free (**www.emisoft.com**). Busca en el disco duro, aunque necesita un poco de tiempo. La versión gratuita viene sin funciones de vacunación. Si te sientes más seguro con protección en tiempo real, compra por 40 euros la versión a-squared Personal.

Como alternativa, recomendamos PestPatrol (**www.pestpatrol.com**). Cuesta unos 40 euros la descarga y unos 50 el CD. Incluye alarmas acústicas y muestra la información detallada de los malware detectados (tipo, tiempo de instalación y forma de actuación). Este programa reconoce los crackers de contraseñas y los escáneres de puertos y se encarga de las cookies que anotan tus visitas y envían información a otros servidores.

Por último, el excelente Winpatrol (**www.winpatrol.com**). Es una herramienta gratuita que te mantiene al corriente de las tareas actuales y de aquellos servicios que se han iniciado en la entrada de registros. Winpatrol ofrece más información que el gestor de tareas o que «msconfig.exe». ■

Direcciones útiles

Contraespionaje gratuito

- **Winpatrol** www.winpatrol.com/download.html
- **a-squared free** www.emsisoft.com
- **a-squared HiJackFree** www.hijackfree.com/en
- **SpywareBlaster** www.javacoolsoftware.com/spywareblaster.html
- **Spybot Search & Destroy** www.safer-networking.org
- **Ad Aware SE Personal** www.lavasoft.com
- **FraudEliminator** www.fraudeliminator.com

Revisión en línea

- **Sygate** scan.sygate.com/pretrojanscan.html
- **Trojanscan** www.windowsecurity.com/trojanscan
- **eTrust Pest Scanner** www.pestpatrol.com/prescan.htm

Información importante sobre malware

- **Database and search engine for unknown file formats** filext.com/index.php
- **Información sobre malware** http://en.wikipedia.org/wiki/Malware
- **Windows applets** www.spywareinfo.com/articles/hijacked/#applets
- **Browser Helper Objects (BHOs) y barra de herramientas** castlecops.com/CLSID.html
- **Explicaciones de servicios Windows** www.processlibrary.com, www.sysinfo.org/startuplist.php (list of start-up functions)

Últimos informes sobre seguridad

- **Boletines para Windows XP** www.microsoft.com/technet/security/

Acaba con los programas espía y los troyanos ocultos en tu PC

A los usuarios nuevos pueden causarles vértigo los peligros en Internet. Pero el sentido común y las herramientas adecuadas son la mejor receta.



Bloquear web peligrosas »

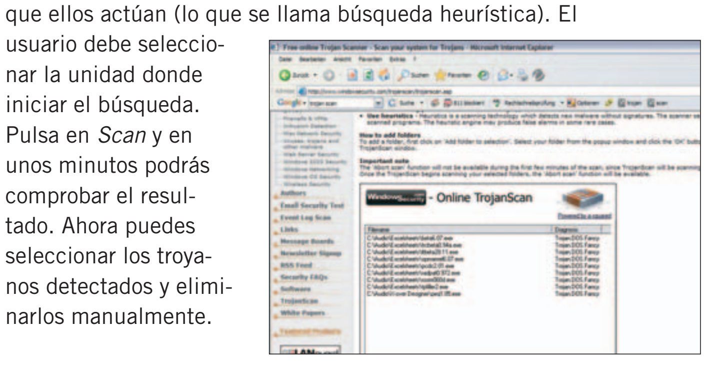
IE-Spyad

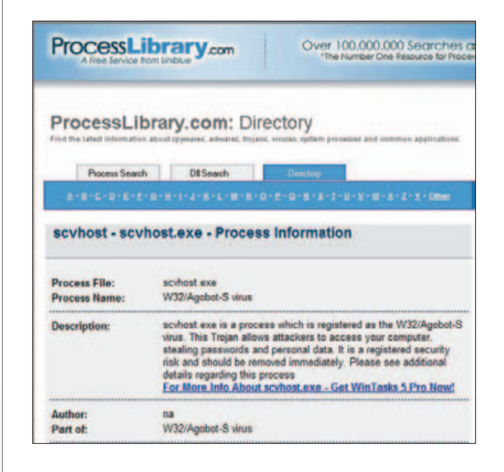
La discreción es la mejor parte del valor. Este el principio por el que IE-Spyad (**netfiles.uiuc.edu/ehowes/www/resource.htm**) trata de minimizar el riesgo de contagio de spyware en tu PC. Este programa sólo trabaja con Internet Explorer (a partir de la versión 4.0) y utiliza un sistema bien simple. Posee una inmensa lista de webs conocidos por difundir spyware y la añade a la lista de sitios bloqueados de Internet Explorer. Si tratas de acceder a una de esas páginas, tanto la instalación de *cookies*, como los controles ActiveX o los *applets* de Java son neutralizados por tu equipo.

Búsqueda *on-line* de spyware »

TrojanScan

Incluso para aquellos que no cuentan con una herramienta anti-spyware, existe la posibilidad de buscar los archivos intrusos en su PC: el truco es utilizar una herramienta desde Internet. En esta tesitura no aconsejamos el uso de de los escáneres de antivirus de renombre como los que abundan en la Web. Los mejor es recurrir a rastreadores especializados en localizar troyanos como es el caso de TrojanScan (que encontrarás en la dirección **windowsecurity.com/trojanscan**). Esta herramienta hace uso de una poderosa rutina de reconocimiento, que se instala como si fuera un control ActiveX de nuestro ordenador. Esta rutina no sólo utiliza firmas para reconocer los troyanos y otros programas *malware*, sino que chequea la forma en que ellos actúan (lo que se llama búsqueda heurística). El usuario debe seleccionar la unidad donde iniciar el búsqueda. Pulsa en *Scan* y en unos minutos podrás comprobar el resultado. Ahora puedes seleccionar los troyanos detectados y eliminarlos manualmente.





Obtener información sobre procesos sospechosos »

ProcessLibrary

No es preciso que cuentes necesariamente con un programa anti-spyware ya que el propio gestor de tareas de Windows (Windows Task Manager) o la herramienta TCPView (**www.sysinternals.com**) evitarán realizar tareas sospechosas que conlleven el contagio. Obviamente, cualquier proceso desconocido no tiene por qué llevar aparejado un troyano… pero existe la posibilidad. En esta situaciones ProcessLibrary (**www.processlibrary.com**) te ayudará a descubrirlo.
Esta base de datos contiene información detallada de procesos dudosos y de las DLLs (Dynamic Link Library) relacionadas. Por tanto, estarás en disposición de borrar o no de tu sistema el software en cuestión.

Internet Explorer seguro »

Enough is enough!

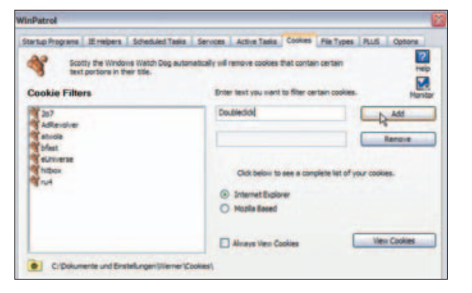
Dado que su cuota de mercado no para de crecer y dadas sus vulnerabilidades, Internet Explorer es el objetivo preferido de los desarrolladores de spyware. Enough is enough! (**netfiles.uiuc.edu/ehowes/www/reource6.htm**) es una herramienta muy útil. Ajusta automáticamente las diferentes configuraciones dentro de Internet Explorer para establecer la máxima seguridad. Esto quiere decir que los sitios sospechosos ya no pueden instalar aplicaciones o *cookies* en nuestro PC. Sin embargo, tendrás que aceptar ciertas limitaciones: el programa es tan restrictivo que no te permitirá visitar webs desconocidas. Para poder ver éstas, tendrás que indicárselo manualmente en la lista de sitios de confianza (*Trusted Sites*).



Defiéndete de las *cookies* »

WinPatrol

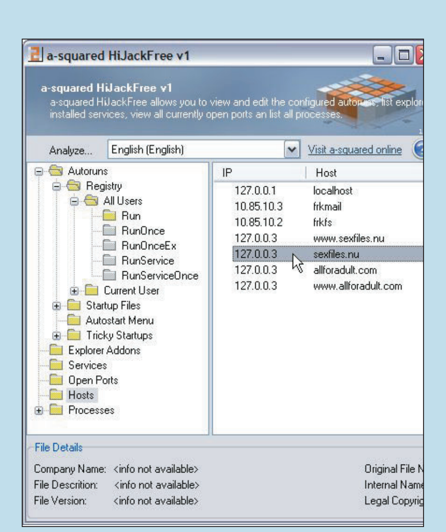
El spyware más frecuente es el que se dedica a rastrear las *cookies*. Estas se utilizan para indagar y analizar las páginas web que visitamos. La información que obtienen de nosotros sirven a las páginas para ofrecernos información personalizada mediante ventanas emergentes. Utilizando el filtro de *cookies* que incluye WinPatrol (**www.winpatrol.com**), evitaremos que esto suceda. Este filtro neutraliza las *cookies* peligrosas pero acepta aquellas que son inofensivas. La lista de filtraciones puede ampliarse de forma que tengamos actualizada nuestra protección.

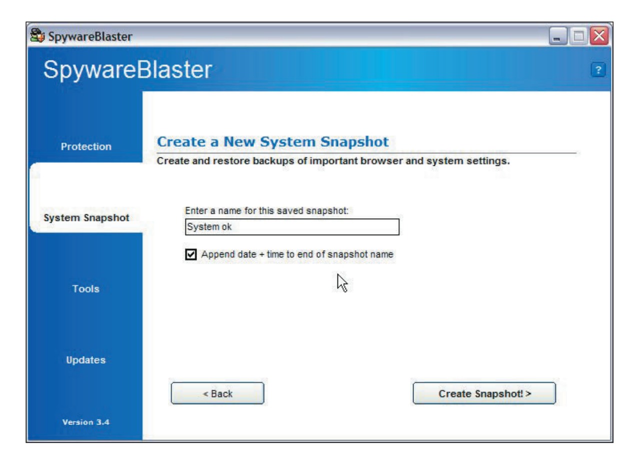


Control de procesos, puertos y servicios »

HiJackFree

Los aficionados a la informática que prefieren buscar por sí mismos spyware en su equipo apreciarán la ayuda de la herramienta HiJackFree. Este programa escanea todas las unidades en busca de programas espía y muestra los resultados. Haz clic en el botón *Analyse* y tu archivo *log* será enviado a un servidor de análisis. El navegador muestra los resultados, de forma que puedes detectar de forma instantánea los posibles peligros. Utilizando el árbol de navegación de HiJackFree en la parte izquierda del panel, puedes situarte rápidamente en la entrada. Ábrela haciendo clic sobre ella. Pulsando ahora sobre él en el panel de la derecha se abrirá el editor relacionado (como Regedit o tal vez Notepad). Ahora puedes realizar los cambios de configuración que desees.





Restaura el sistema al punto anterior a la infección »

SpywareBlaster

Si tu ordenador ha caído víctima de una ataque de spyware, puede que seas capaz de eliminar al causante del daño, pero a menudo tu navegador y sistema no estarán en situación operativa. Esto significa por desgracia que hay que reinstalar todo de nuevo. Por suerte, esto es inevitable. Utiliza la función *Snapshot* de SpywareBlaster (**www.javacoolsoftware, com/spywareblaster.html**). Esta herramienta salva una imagen de las configuraciones de tu sistema y de tu navegador, Su uso es muy fácil. Cuando estés seguro que tu sistema está limpio, salva la configuración con la opción *System Snapshot/Create a new System Snashot*. Después de un ataque, restaura la copia de seguridad seleccionando *System/Snapshot/Restore System to Saved Snapshot Point*.

Utiliza Windows para rastrear el espionaje

C:\WINDOWS\WIN.INI
C:\CONFIG.SYS
C:\AUTOEXEC.BAT
C:\WINDOWS\SYSTEM.INI
; for 16-bit app support
[drivers]
wave=mmdrv.dll
timer=timer.drv
[mci]
[driver32]
[386enh]

1 **Revisa los archivos .ini del sistema para ver si tiene entradas indeseadas.**

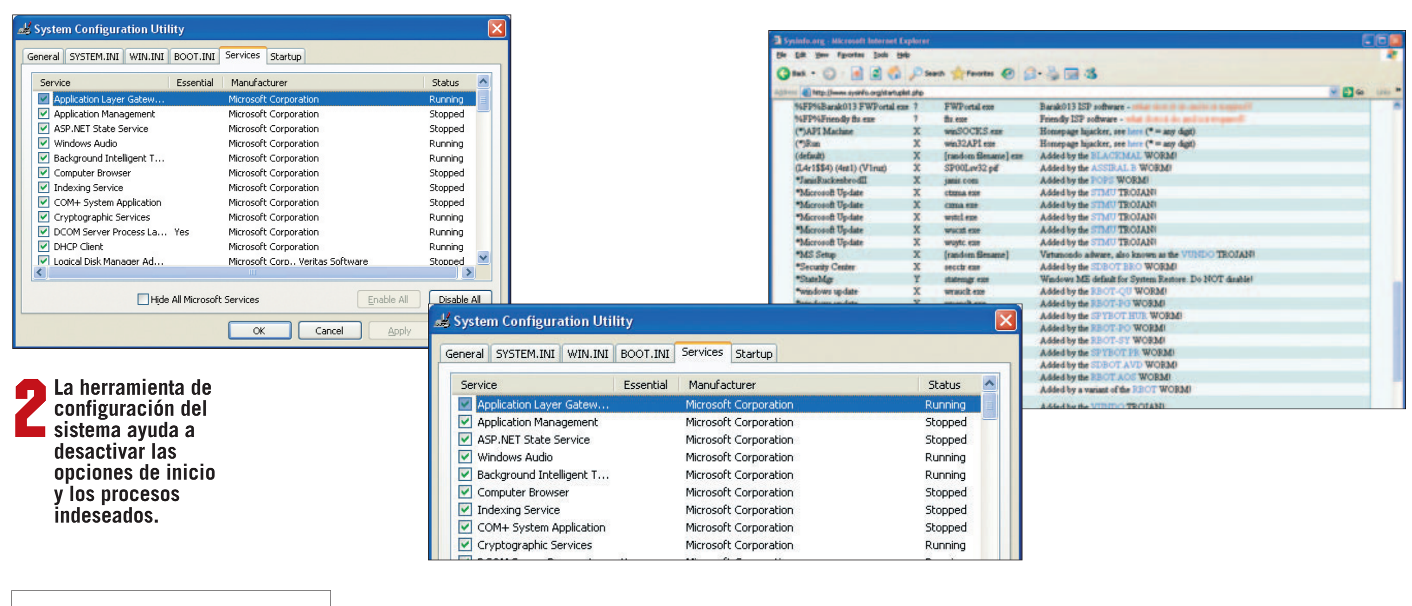
Cada vez que utilizas Internet, corres peligro de infectarte de ciberparásitos. Confiar demasiado en tu antivirus puede ser un gran error, porque estas aplicaciones, que funcionan muy bien en lo que respecta a la localización de virus, no son tan buenas a la hora de reconocer a los troyanos y a los programas espías. Si no tienes un software especializado, puedes utilizar las funciones propias de Windows para determinar si se ha introducido un peligroso troyano en tu sistema. Antes de que comiences a buscarlo, asegúrate de que el explorador de Windows muestra todos tus archivos, incluidos los nombres de la extensión. Puedes hacer esto en *Ver/Configuración avanzada* dentro de *Herramientas/Opciones de carpeta*. Las casillas *Ocultar las extensiones de archivo para tipos de archivo conocidos* y *Ocultar archivos protegidos del sistema operativo* no deben estar marcadas. Por el contrario, las casillas *Mostrar el contenido de las carpetas del sistema* y *Archivos y carpetas ocultos/Mostrar todos los archivos y carpetas ocultos* deberían estar marcadas.

1 Archivos de arranque de Windows

El propósito de un troyano es recoger información de tu sistema y transmitirla a un atacante externo. Por consiguiente, necesita actuar en la sombra, haciendo su rastreo. Empieza la caza buscando, entre los archivos de arranque, alguno que pueda parecer sospechoso. La mayoría de los modernos troyanos no utilizan este sistema porque les hace demasiado vulnerables. Pero no está de más asegurarte antes de buscar en cualquier otro lado. *Ejecutar/sysedit* arranca el editor, que abre los cuatro archivos de arranque más importantes: «autoexec.bat», «config.sys», «system.ini» y «win.ini». En Windows, revisa «win.ini» con los parámetros *Load=* y *Run=*. En «system.ini», echa un vistazo a la sección de arranque. Por ejemplo, si encuentras una línea del tipo «shell=Explorer.exe Task_bar.exe», has detectado el troyano Subseven. En este caso, elimina inmediatamente el «Task_Bar.exe» de esta entrada. En Windows 98, deberías asegurarte de mirar «config.sys» para entradas posteriores a *Device=*, *Install=*, *Devicehigh=*, *Installhigh=* y *Shell=*.

2 Revisa el Registro

A continuación, mira si algún troyano se ha colado en el registro, con la intención de ser iniciado automáticamente cada vez que arrancas el ordenador. Utiliza *Ejecutar/Msconfig -6* para iniciar la utilidad de configuración del sistema. Puedes utilizar esta ruta para detectar y desactivar la mayoría de los troyanos. Msconfig es mucho más fácil de usar que el editor de registros. Aquí ves qué aplicaciones empiezan por las claves de ejecución en las secciones *HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion y HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion*. Vacía las entradas o enlaces a archivos desconocidos como «COMDRIV32» o «loadkk.exe» que parezcan sospechosos. Ten en cuenta que el malware utiliza a menudo nombres que pueden confundirse fácilmente con un inocente proceso del sistema. Por ejemplo, «scvhost.exe» es un nombre de proceso utilizado por numerosos virus y troyanos. Este nombre es casi idéntico a «svchost.exe»,



2 **La herramienta de configuración del sistema ayuda a desactivar las opciones de inicio y los procesos indeseados.**

```
C:\Documents and Settings\TEST>netstat -a

Active Connections

  Proto  Local Address            Foreign Address        State
  TCP    testknecht:epmap         testknecht:0           LISTENING
  TCP    testknecht:microsoft-ds  testknecht:0           LISTENING
  TCP    testknecht:netbios-ssn   testknecht:0           LISTENING
  TCP    testknecht:1028          testknecht:0           LISTENING
  UDP    testknecht:microsoft-ds  *:*
  UDP    testknecht:isakmp        *:*
  UDP    testknecht:1034          *:*
  UDP    testknecht:1050          *:*
  UDP    testknecht:4500          *:*
  UDP    testknecht:ntp           *:*
  UDP    testknecht:netbios-ns    *:*
  UDP    testknecht:netbios-dgm   *:*
```

3 Netstat averigua los procesos que están conectados a Internet.

uno de los procesos de Windows más importantes. Quita la marca de la casilla que está frente al nombre para desactivar esta entrada. Si no estás completamente seguro, echa un vistazo a **www.sysinfo.org/startuplist.php** para información adicional sobre procesos Windows. No olvides anotar el nombre del archivo y la ruta de las aplicaciones sospechosas. Haz clic en la pestaña de servicios. Aquí encontrarás algunos servicios de vendedores desconocidos. Estos servicios no tienen por qué ser peligrosos. Utiliza *Inicio/Panel de control/Herramientas de administración/Servicios* para averiguar más sobre ellos.

Abre las *Propiedades* de un servicio sospechoso en el menú emergente: obtendrás información adicional y la ruta del archivo «.exe». Si todavía tienes la impresión de que este servicio es sospechoso, podrás volver y eliminarlo.

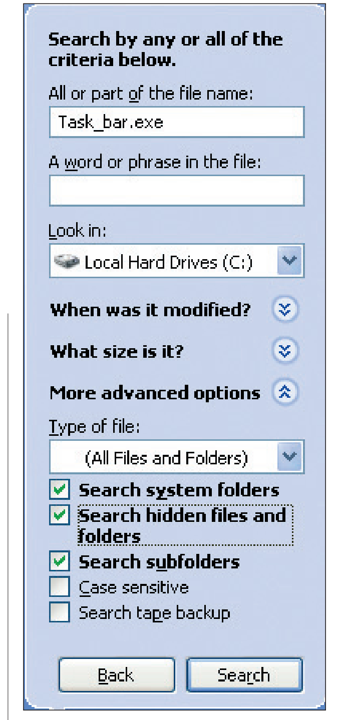
Por último, vamos a necesitar el editor del registro. Inícialo con el ya habitual *Ejecutar/regedit* y navega por la clave de registro *HKEY_CLASSES_ROOT\exefile\shell\open\command*. Aquí deberías encontrar una entrada *"%1"%**. Si hubiese alguna otra entrada antes que el uno, incluido un archivo «.exe», tu ordenador podría estar infectado. Quita la parte de la entrada sospechosa, pero deja la entrada del uno.

3 Revisa procesos y puertos

Los troyanos transmiten información sigilosamente, pero siempre dejan un rastro. Para enviar algo, necesitan abrir uno o varios puertos de comunicación. Puedes comprobar esto fácilmente. Reinicia tu sistema. Abre la consola con Ejecutar/cmd y después introduce el comando "netstat –o". Windows muestra todas las comunicaciones activas en el host, incluidos sus puertos. Todas las conexiones (TCP o UDP) a servidores desconocidos son sospechosas. Si ves una conexión a un servidor IRC cuando tú no has estado chateando, entonces puedes sospechar. Si no estás seguro de lo que significa la salida Netstat, utiliza la lista de puertos Commodon Communications para averiguarlo (**www.commodon.com/threat/index.htm**). Usa el gestor de tareas para acabar con todos los procesos peligrosos de un plumazo. Al utilizar Netstat con el parámetro «-o»; la salida incluye el PID, por lo que es fácil identificarlos y eliminarlos en el gestor de tareas. Anota el nombre de los archivos y el lugar de localización de los procesos eliminados. Espera un poco para ver si el gestor de tareas funciona si el proceso se inicia de nuevo. Si esto ocurre, desconecta inmediatamente el ordenador de Internet.

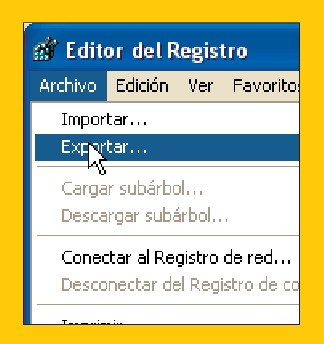
4 Elimina el troyano

Finalmente, revisa tus notas con los procesos y aplicaciones sospechosas (estás a punto de acabar con estos parásitos). El gestor de tareas y el editor de registros localizan el malware, por supuesto, pero no confíes sólo en ellos: suele suceder que un archivo se guarda en varios sitios distintos del ordenador. Averigua si hay copias con el buscador de Windows. Cambia la extensión del archivo de todas las entradas encontradas, de «.exe» a «.txt». De esta forma, dejarán de ser archivos ejecutables; es decir, dejarán de ser peligrosos. Sin embargo, como siguen en tu PC, podrán ser siempre restaurados como ejecutables, en caso de que te hubieses confundido al identificarlos como peligrosos y fueran en realidad archivos importantes.



4 La función de búsqueda de Windows ayuda a rastrear a los espías.

Trabajando con el registro



Trabajar dentro del registro de Windows es delicado. Si eliminas una clave importante o introduces un dato falso, tu sistema no volverá a funcionar bien nunca más: en el peor de los casos, ni siquiera conseguirá arrancar. Por tanto, cada vez que hagas algún cambio en el registro, deberías hacer una copia de seguridad de tus configuraciones. Para hacer esta copia, elige la opción Exportar **del menú** Archivo del editor de registro **y selecciona el lugar donde quieres guardar ese archivo de seguridad.**

Preguntas y respuestas

¿Navegas por Internet sin ninguna protección contra posibles malware, troyanos y virus? Entonces es como si nadaras en un agua llena de tiburones.

? Sigo oyendo cosas sobre malware, virus, troyanos, puertas traseras y registradores de teclas. Me gusta mucho Internet pero... ¿debería saber algo más?

! Estos términos se refieren a distintos tipos de software maligno (o malware)... que actúan de distinta forma y con diferentes objetivos. «Malware» es el término genérico que engloba a cualquier programa diseñado para dañar tu ordenador y su contenido.
Por otro lado, un virus es un programa capaz de replicarse y expandirse por la red. Generalmente, un virus dañará un PC infectado eliminando ciertos archivos o todo el disco duro. Un virus suele empezar por la interacción del usuario que, por ejemplo, ejecuta un archivo «.exe». Los gusanos son una subespecie de virus y pueden infectar un ordenador sin que ni siquiera haya interacción por parte del usuario.
Un caballo troyano (se suele llamar simplemente troyano) es, como su nombre indica, un programa que oculta su verdadero propósito. Por ejemplo, un troyano puede pretender ser un juego gratuito, mientras que su verdadero trabajo consiste en fisgonear en la información secreta de tu sistema. Para conseguirlo, el parásito se instala en el disco duro y transmite información sin que tú lo sepas. A diferencia de los virus, los troyanos no se clonan por sí solos.
Todos los troyanos y algunos virus contienen un módulo de puerta trasera. Esto permite a un atacante externo controlar tu sistema (y dañarlo, si lo desea).
Por último, pero no por eso menos importante, los registradores de teclas son unos programas sencillos pero tremendamente peligrosos. Su propósito es el de registrar todas las pulsaciones del teclado y enviar el protocolo a un atacante externo sin que tú puedas darte cuenta. Es una forma de conseguir contraseñas, datos sobre cuentas bancarias y números de tarjetas de crédito.

Si quieres evitar que los extraños fisgoneen en tu ordenador no tendrás más remedio que instalar lo último en seguridad, como SpywareBlaster.

? ¿Cómo funciona un troyano?

! A diferencia de los virus, los troyanos tienen dos partes, una cliente y una servidor. La parte servidor se instala en tu sistema sin tu conocimiento. Cada vez que arrancas el PC, el servidor comienza a funcionar. Cuando está en ejecución, abre puertos de comunicación, normalmente un puerto TCP aunque también puede abrir un UDP. Con él consigue que un atacante externo tenga acceso a tu ordenador y lo controle desde fuera. Sin embargo, antes que esto pueda ocurrir, necesita saber la dirección IP actual de la víctima. Una tarea que también realiza el troyano, que transmite este dato por correo electrónico, ICQ o IRC al atacante sin que tú te enteres.

? ¿Cuál es el peligro de un troyano?

! Con un troyano, el atacante obtiene acceso a tu ordenador y a toda la información que contiene. Por ejemplo, si lo desea, puede eliminar datos de tu ordenador. Imagina que estos datos se refieren a un proyecto empresarial: la pérdida podría ocasionar un serio daño financiero. Otra amenaza es la de registrar tus pulsaciones. De esta manera, un atacante puede fisgonear en tu cuenta o en los datos de tu tarjeta de crédito y comprar por Internet con tu dinero. Los troyanos pueden también descubrir contraseñas y direcciones de correo electrónico.
Otro riesgo es el abuso de tu ordenador para actividades ilegales. Por ejemplo, los hackers podrían usarlo para ataques DDoS (*Distributed Denial of Services*), un método clásico para entrar y deshabilitar las redes de las grandes empresas.

? ¿Puede mi antivirus protegerme de estos troyanos?

! Un antivirus sólo no puede protegerte. Te recomendamos que utilices un programa de contraespionaje o, mejor todavía, varios de estos programas. Esta política incrementará las posibilidades de éxito. Existen buenas utilidades gratuitas como a-squared (**www.emsisoft.com/com/software/free**), Spybot Search&Destroy (**www.safernetworking.org**) y SpywareBlaster (**www.javacoolsoftware.com/spywareblaster.html**).

WLAN de la A a la Z

Si quieres entender la tecnología WLAN, debes conocer las más habituales expresiones técnicas y acrónimos. Todos los términos relevantes aparecen en este glosario.

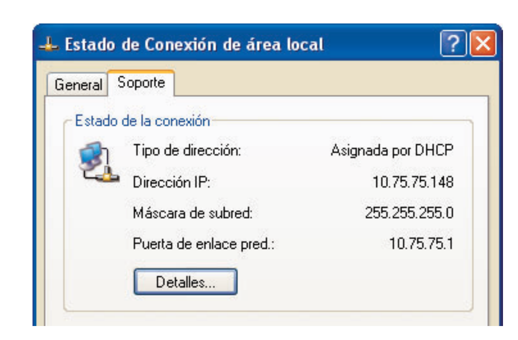


1 Los dispositivos con el logo Bluetooth utilizarán este método de comunicación de datos.



2 La tecnología Intel Centrino combina la tecnología WLAN con los potentes procesadores Pentium para portátiles.

3 La dirección IP local en una red WLAN será asignada por un servidor DHCP.



ADSL *Asymetric Digital Subscriber Line* es la forma más común de banda ancha. Se le dice asimétrica porque el flujo de subida y el de bajada no van a la misma velocidad.

ANCHO DE BANDA El ancho de banda indica la capacidad de una conexión de comunicación. Cuanto mayor ancho de banda, más datos se pueden transmitir al mismo tiempo.

BLUETOOTH Se trata de un estándar inalámbrico de comunicación, con una entrada de datos de hasta 1 Mbit/s. Su alcance de transmisión es mucho más corto que con WLAN, pero ambos no se interfieren al transmitir datos. [1]

CENTRINO Introducido por Intel, Centrino es un combinado de procesador, placa base y WLAN para ordenadores portátiles. Se basa en un procesador Pentium M y soporte de red inalámbrica Intel Pro/Wireless 2100 (IEEE 802.11b). Centrino debería garantizar el menor gasto posible de batería. [2]

CSMA/CA *Carrier Sense Multiple Access/Collision Avoidance* es un método para acceder a distintos clientes de una red con el mismo medio de transmisión. Este método es utilizado principalmente en WLANs, pero también se presenta en otras tecnologías, como ISDN.

DHCP *Dynamic Host Configuration Protocol* Con él, las direcciones IP se asignarán automáticamente al ordenador. Si entras en Internet directamente, sin una red doméstica de por medio, el servidor SHCP de tu proveedor de Internet te proporciona una dirección IP. Si accedes a Internet a través de una red privada, la dirección IP te la proporciona el router. Esta dirección es dinámica, lo que significa que cambia cada vez que te conectas.

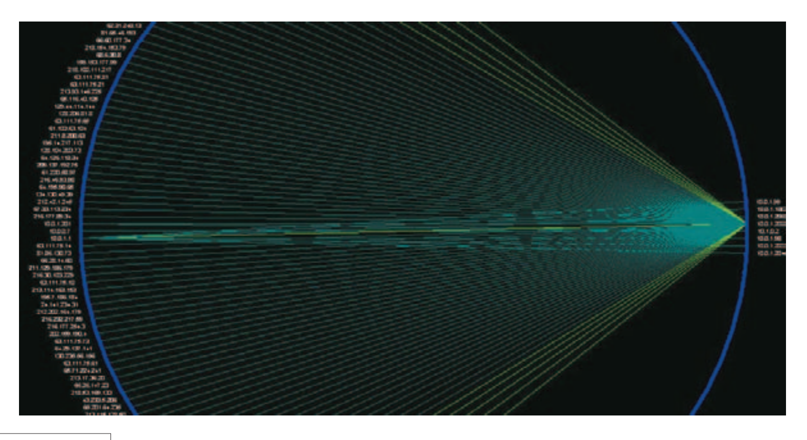
DIRECCIÓN IP: La dirección IP es como el número en la puerta de tu ordenador en Internet; esto es, la dirección para la entrada de paquetes. La dirección IP consiste en cuatro cifras de tres dígitos cada una, con la primera de ellas describiendo la dirección de la red y las cuatro, en conjunto, asignando el número del propio PC. [3]

DIRECCIÓN MAC *Media Access Control* Es la dirección hardware de cada dispositivo de red (switch, tarjeta de red, etc.). Es necesario para la identificación inequívoca del dispositivo dentro de la red. Es única en todo el mundo. Se configura al poner en marcha la máquina y nunca cambia.

DNS Abreviatura de *Domain Name System.* Este proceso traduce el nombre del PC en sus direcciones IP y viceversa.

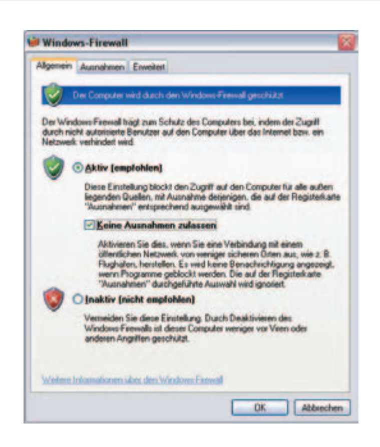
FIREWALL O CORTAFUEGOS Un firewall protege un PC o una red local de ataques provenientes de Internet. Casi todos ellos operan con un filtro de paquetes, que comprueba las direcciones IP y los números de puerto de los paquetes de datos de entrada y salida, y los filtra de acuerdo a normas preestablecidas. Los routes WLAN actualizados generalmente tienen un cortafuego integrado, que sirve para bloquear los paquetes de datos peligrosos. Incluso Windows XP SP2 tiene un cortafuegos incorporado, pero es un poco rudimentario. Los dos firewalls, uno hardware y otro software, pueden trabajar juntos. Dos software no pueden hacerlo en un mismo sistema. [4]

7 El gusano Nimda establece contacto con sus víctimas, en este caso a través de un programa especial quer muestra una vista radial de todas las direccioines IP que han sufrido contacto.



8 Los hotspot públicos son ofrecidos por algunos restaurantes, aeropuertos y estaciones de tren.





4 Windows XP instala un cortafuego rudimentario con Service PAck 2. Puedes desconectarlo si has planeado una alternativa.



5 FireWire permite una mayor fluidez de datos entre PC, cámara, disco duro y otros dispositivos.

6 Las gateways son responsables de la distribución de los datos de la red a los clientes.



FIREWIRE Este estándar fue inventado por Apple. Se trata de un puerto con unos ratios de transferencia muy altos. Permite conectar hasta 16 dispositivos externos, desde cámaras a discos duros. [5]

FRAGMENTACIÓN Si estás enviando un paquete IP, puede suceder que el servidor de partida tenga un valor de MTU más bajo, de modo que el paquete no pueda pasar. En ese caso, será fragmentado (dividido en piezas menores).

GATEWAY Se trata de una interfaz entre dos redes de ordenadores. En tu WLAN, el router hace las funciones de gateway entre la red local e Internet. [6]

GUSANO Pequeño programa que se introduce en una red a través de agujeros de seguridad. Los gusanos se transmiten por *e-mail,* programas de mensajería instantánea o chat, o al compartir ficheros. El objetivo de los gusanos es expandirse rápidamente. Al contrario que los virus, su misión rara vez es explícitamente destructiva. [7]

HOST Son ordenadores de gran capacidad y servidores que proveen servicios personalizados a las estaciones de trabajo conectadas en una red.

HOTSPOT Un *hotspot* es un punto de acceso inalámbrico público. Cada hay más de ellos instalados en lugares públicos y en hoteles, restaurantes, aeropuertos y estaciones de tren. Las autoridades de Filadelfia, Estados Unidos, están planeando transformar toda la ciudad en un *hotspot* gigante, ofreciendo acceso para todos. [8]

IEEE 802.11 La etiqueta IEEE 802.11 denota el estándar de la industria para la comunicación de redes inalámbricas, codificadas por el Institute of Electrical and Electronics Engineers (IEEE) en su primera versión, que data de 1997.

IP Internet Protocol: El protocolo de Internet es un sistema responsable de la correcta distribución de paquetes de datos en Internet.

ISDN Integrated Services Digital NetworkAcelera la transmisión de datos digitalizándola, en lugar de tranasformarla en señales analógicas.

MIMO *Multiple input Multiple Output* En una red inalámbrica, es un método que optimiza la velocidad de transmisión usando un conjunto de antenas y que asegura un flujo de datos constante. Algunos routers actualizados ya utilizan MIMO. [9]

MODEM Se trata de un acrónimo de Modulador/Demodulador. El módem funciona como un conversor de señal: cambia la señal digital en analógica y viceversa.

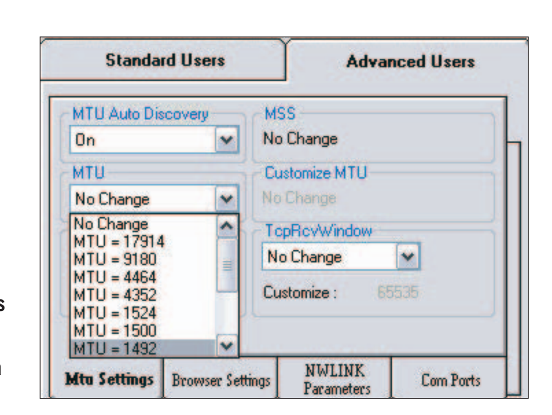
MSS *Maximum Segment Size* Mientras la abreviatura MTU designa el tamaño de los paquetes IP, MSS designa el tamaño de la cuota de datos de los paquetes TCP que un PC puede manejar.

MTU *Maximum Transmission Unit* Designa el mayor paquete de datos IP que pueden ser transportados sin fragmentar. Un valor MTU alto significa mayor velocidad. El valor máximo para una interfaz Ethernet es 1500, pero en la práctica es más aconsejable 1492 para evitar pérdida



9 Los routers MIMO disponen de múltiples antenas para garantizar un flujo de datos estable.

10 Puedes cambiar el valor MTU del Registro. Pero es más sencillo permitir que se encargue de esta tarea algún programa especializado como Befaster.



WLAN from A to Z

11 Se puede comprobar el estado del servidor realizando un ping desde el Símbolo de sistema.

```
D:\WINDOWS\system32\cmd.exe
Microsoft Windows XP [Version 5.1.2600]
(C) Copyright 1985-2001 Microsoft Corp.

D:\Dokumente und Einstellungen\Oliver>ping

Ping                    [217.        ] mit 32 Bytes Daten:

Antwort von 217.        : Bytes=32 Zeit=64ms TTL=56
Antwort von 217.        : Bytes=32 Zeit=62ms TTL=56
Antwort von 217.        : Bytes=32 Zeit=61ms TTL=56
Antwort von 217.        : Bytes=32 Zeit=61ms TTL=56

Ping-Statistik für 217.        :
    Pakete: Gesendet = 4, Empfangen = 4, Verloren = 0 (0% Verlust),
Ca. Zeitangaben in Millisek.:
    Minimum = 61ms, Maximum = 64ms, Mittelwert = 62ms

D:\Dokumente und Einstellungen\Oliver>
```



12 Los puntos de acceso se aseguran de que los clientes de la red puedan navegar via ADSL.

de datos.[10]

PING Una manera de comprobar el tiempo de reacción delservidor o el cliente. Envía paquetes de datos pequeños y mide el tiempo de transferencia requerido. [11]

PPP *Point-to-Point Protocol* indica una conexión punto a punto entre tu servidor ISP y tu PC; es empleado por el proveedor. Muchos proveedores de ADSL utilizan PPP sobre Ethernet (PPPoE) para los accesos. Los paquetes IP forman paquetes PPP y son transmitidos vía Ethernet.

PUNTO DE ACCESO Un punto de acceso es un dispositivo que conecta la red inalámbrica con redes de cable, o redes de comunicaciones inalámbricas y los terminales. En redes WLAN el punto de acceso permite el uso de ADSL por parte de tpdps los usuarios y dispositivos conectados. [12]

PUERTO Todo sistema operativo emplea los así llamados puertos, de modo que múltiples programas puedan enviar y recibir datos en la misma conexión de red. Son como las puertas de una casa: si todas están cerradas no habrá acceso, pero con cada puerta abierta el peligro de que los datos sean espiados o saboteados aumenta. [13]

ROUTER Se encarga de distribuir los paquetes de datos entre dos redes separadas física o lógicamente. El router determina la major ruta para que un paquete de datos llegue al receptor.

TTL *Time to Live* Todos los paquetes de datos contienen información acerca de cuánto deben permanecer en la Red, llamada TTL. Si no es posible realizar la entrega en ese tiempo, será devuelta y no alcanzará el ordenador de destino. Sirve para evitar que paquetes inútiles vaguen indefinidamente por Internet.

TCP *Transmision Control Protocol TCP/IP* es un conjunto de protocolos desarrollados en los 70 en los Estados Unidos por WAN (World Area Network) y se utiliza también en redes locales. El trabajo de TCP es establecer las conexiones y el flujo de datos entre cada cliente de la red. IP organiza y envía los datos.

TLD *Top Level Domain* Indica el nivel más alto en la jerarquía del dominio y contiene los dominios por país (como «.es» o «.mx») o los genéricos (como «.com», «.net», etc.).

WIMAX *Worldwide Interoperatibility for microwave access* Nuevo estándar (IEEE 802.16) para redes inalámbricas regionales que aún no ha llegado al mercado. WIMAX puede tomar el puesto de WLAN en todos los lugares con un alcance de hasta 50 km y un ratio de transferencia de datos de hasta unos teóricos 109 Mbits/s. WIMAX rquiere contacto visual entre el remitente y el receptor para trabajar mejor. [14]

WLAN *Wireless Local Area Network* El protocolo WLAN define la forma de compartir datos en redes inalámbricas. Actualmente hay dos estándares: 802.11g tiene unratio de transferencia de datos de hasta 54 Mbits/s; el más antiguo 802.11b soporta 11 Mbits/s. El próximo 802.11n debería ver incrementada diez veces la velocidad de transmisión.

Dienst	Port-Nr.
Ping	7
FTP	21
Telnet	23
SMTP	25
DNS	53
TFTP	69
Gopher	70
WWW	80
POP3	110
NNTP	119
NetBIOS	139
SNMP	161
HTTPS	443
Oracle	1525
MySQL	3306
IRC	6667

13 Windows reserva puertos específicos para servicios online y tareas de red.

14 WIMAX debería tener un radio de alcance de 50 km, siempre que haya contactovisual.

